

인공지능보안

일 정 2023년 8월 10일(목) 09:30~17:30

진행방식 온·오프라인 병행

장 소 한국인터넷진흥원 판교기업지원허브 4층 정보보호클러스터 컨퍼런스룸
(경기도 성남시 수정구 대왕판교로 815)

주 최 한국정보보호학회



초대말씀

알파고에서 챗GPT까지 인공지능 기술은 이 시대의 키워드로서 모든 분야에 혁신을 주도하고 있습니다. 보안 분야에서도 예측형 인공지능 기술을 다양한 산업 현장 실무에 활용하는 사례가 증가하고 있으며, 최근에는 생성형 인공지능 기술에 대한 활용과 그로 인한 업무 혁신에 대한 기대감이 높아지고 있습니다. 하지만 보안 측면에서 예측형과 생성형 인공지능 기술에 내재 되어 있는 한계성과 불확실성에 대한 우려감과 향후 발생이 예상되는 전례 없는 인공지능 악용 사례에 대한 경계심 또한 커지고 있습니다. 이에 본 단기강좌에서는 보안 관점에서 인공지능 기술과 관련된 세 가지 주요 이슈들-신뢰, 생성, 활용-에 대해 다루고자 합니다. 학계와 산업계를 대표하는 인공지능 전문가들과 보안 전문가들의 튜토리얼 및 전문 강연을 통해서 인공지능보안에 대한 근본적 고찰과 미래 방향성을 제시하고자 합니다. 인공지능보안에 관심 있으신 많은 분들의 참여를 기대합니다.

행사 개요

- 일 정 : 2023년 8월 10일(목) 09:30~17:30
- 진행방식 : 온/오프라인 병행
- 장 소 : 한국인터넷진흥원 판교기업지원허브 4층 정보보호클러스터 컨퍼런스룸(경기도 성남시 수정구 대왕판교로 815)
- 주 최 : 한국정보보호학회

학회장

- 조 직 위 원 장 : 원유재 교수(충남대)
- 운 영 위 원 장 : 서대희 교수(상명대)
- 프로그램 위원장 : 윤명근 교수(국민대)

강의 내용

시간	발표주제	발표자
09:30~10:30	생성형 AI와 보안 (튜토리얼)	이재구 교수(국민대)
10:30~10:40	휴식	
10:40~11:20	Graph Neural Network 기반 침해공격 분석 및 해석	이태진 교수(호서대)
11:20~12:00	금융분야 AI 보안 가이드라인	송은지 수석(금융보안원)
12:00~13:00	점심 및 휴식	
13:00~14:30	거대언어모델과 보안: ChatGPT에서 LLM까지 (튜토리얼)	고우영 선임(국가보안기술연구소)
14:30~14:40	휴식	
14:40~15:20	최신 생성모델 기반의 프라이버시 보호 기술	배호 교수(이화여대)
15:20~16:00	Explainable AI: Foundations and Applications	김진규 교수(고려대)
16:00~16:10	휴식	
16:10~16:50	자동화된 보안관제를 위한 AI/ML 학습데이터 및 탐지모델 구축 사례	이준 박사(한국과학기술정보연구원)
16:50~17:30	인공지능보안 분야 좋은 논문 작성을 위한 제언 - 사례중심	양대현 교수(이화여대)

등록안내

구분	교육비
일반	250,000원
학생	150,000원
시니어(63세 이상)종신회원	무료

- 사전등록마감 : 2023.8.3.(목) 오후 6시까지
- 학회홈페이지(www.kiisc.or.kr)→ 학회행사→ 사전등록 바로가기→ 2023 단기강좌
- 무통장 입금 시 : 국민은행 754-01-0008-146 (예금주 : 사)한국정보보호학회)
- 입금명은 필히 [행사명 첫 글자+등록자성함]으로 기재해 주시기 바랍니다.
예) 2023 단기강좌 등록 홍길동 → “단홍길동”기재
- 시니어 무료등록은 학회 종신회원으로 1961년 12월 31일 이전 출생자에 한합니다.
- 학생은 다른 소속이 없는 전일제 학생(학부생 및 대학원생)에 한합니다.
- 신용카드 결제 시 계산서 발급이 불가합니다. (부가가치세법 시행령 제57조)
- 계산서 신청 시, 익일 안으로 등록하신 이메일로 청구용 계산서가 발행 됩니다. 영수용 계산서가 필요하신 경우, 사전에 학회로 연락 바랍니다.
- 주차권은 지원 되지 않습니다.

문의처: 한국정보보호학회

- 전화 : 02-564-9333~4 (내선1)
- 이메일 : kiisc3@kiisc.or.kr

