2021.07.07
— 07.09

AI 보안 워크샵 2021

온라인 실시간 중계

YouTube 한국정보보호학회

홍천 비발디 파크 ,
타워 B동 지하 라벤더 1 회의장

주최 | 한국정보보호학회 주관 | 한국정보보호학회 AI보안연구회, 숭실대학교 AI보안연구센터

Program

2021.7.7 (Wed) (▶ 온·오프라인 병행)

시간	좌장	내 용	연사
		Tutorial	
15:00~17:00	**권태경 교수**(연세대)	심층인공신경망 구조 및 적대적 공격에 강인한 구조	**김현우 교수**(고려대)
17:00~17:10		Coffee Break	
		AI보안연구센터 Session	
17:10~17:30	**한명묵 교수**(가천대)	AI 보안 연구센터 성과 현황	**정수환 교수**(숭실대)
17:30~18:10		창의자율과제 중간 발표 및 평가	**과제책임자** (5인)
18:10~19:00		Reception	

2021.7.8 (Thu) (▶ 온·오프라인 병행)

시 간	좌 장	내 용	연 사
		Session 1: AI Threat	
10:00~10:50	**백윤흥 교수**(서울대)	언어 인공지능의 발전과 신뢰성**(trustworthiness)**	**임준호 박사**(ETRI)
10:50~11:40	**문대성 실장(ETRI)**	전이학습과 지식증류를 활용한 딥페이크 동영상 탐지 기법 연구	**우사이먼 교수**(성균관대)
11:40~13:00		Lunch	
		Session 2: Security for AI	
13:00~13:50	**윤한준 실장(NSR)**	심층학습모델 워터마킹 기법과 공격 방법	**손수엘 교수**(KAIST)
13:50~14:40	**기주희 박사(IITP)**	**Adversarial Example** 방어 기술 연구 소개	**최대선 교수**(숭실대)
14:40~15:00		Coffee Break	
		Session 3: AI for Security	
15:00~15:50	**박기웅 교수**(세종대)	**Learning on Graphs**	**이재구 교수**(국민대)
15:50~16:40	**한동국 교수**(국민대)	제어시스템 보안위협 탐지기술 개발을 위한 머신러닝 활용 경험	**윤정한 박사**(NSR)
16:40~17:00		Coffee Break	
		패널 토의	
17:00~18:00	**정수환 교수**(숭실대)	**Trustworthy AI**	강병훈 교수(KAIST) 김의탁 소장(이스트시큐리티) 최대선 교수(숭실대)

2021.7.9 (Fri) (▶ 오프라인)

시 간	좌 장	내 용	연 사
		AI보안연구회 운영위원회	
10:00~12:00	**정수환 교수**(숭실대)	AI보안연구회 향후 활동 방향 및 연구 주제 토의	
12:00~		Closing	

위치 및 교통 안내

[홍천 비발디 파크]

구분	특징
오시는 길	잠실에서 77km, 약 1시간 소요(승용차기준)
주소	강원도 홍천군 서면 한치골길 262
연락처	TEL : 1588-4888 | FAX : 033) 434 - 8020

*무료셔틀 이용

- ▶ 소노벨 비발디파크 홈페이지에서 예약 가능
- ▶ 셔틀버스 문의 전화 : 033) 439-7695