한국정보처리학회 2025년 제 1 차 단기강좌

인공지능 기반 최신 보안기술

25.04.04. FRI

강남역 YBM the Biz 401호 (온/오프라인 병행개최)

사전등록 마감일 4/3(목)까지

조직구성

학 회 장	**황종성** 원장(한국지능정보사회진흥원)
수 석 부 회 장	**박능수** 교수(건국대학교)
담 당 부 회 장	**김경백** 교수(전남대학교)
운 영 위 원 회	**김경백** 교수(전남대학교), **이강원** 교수(세종대학교), **이문규** 교수(인하대학교)
프로그램위원장	**이문규** 교수(인하대학교)
프 로 그 램 위 원	**권현수** 교수(인하대학교), **김형식** 교수(성균관대학교), **서승현** 교수(한양대학교), **이용우** 교수(인하대학교)

강좌소개

최근 인공지능과 양자컴퓨팅 등의 기술 발전으로 정보 및 컴퓨팅 분야의 패러다임이 급격히 변화하고 있습니다. 보안 분야에서도 AI를 활용해 보안 분야의 난제를 해결하는 기술, AI 모델과 학습 데이터를 안전하게 보호하는 새로운 보안 기법, 생성형 AI를 실세계에 안전하게 적용하는 기술, 그리고 양자컴퓨팅 기반 공격에 대응하는 새로운 암호 알고리즘 개발 및 적용 등 다양한 연구가 활발히 진행되고 있습니다. 본 강좌에서는 최근 보안 분야의 주요 국제 학술대회 및 저명 학술지에 발표되었거나 발표 예정인 논문을 중심으로 보안 분야 최신 연구 동향을 살펴봅니다. 이를 통해 미래 보안 기술의 발전 방향을 모색하고, 보안 전문가들과의 교류가 이뤄질 수 있는 장이 되기를 기대합니다.

일정표

시간	발표 주제 및 요약 내용	강사
09:50~10:00(10')	사 회 **이문규** 교수(인하대)	
	인사말 **황종성** 회장(한국정보처리학회, NIA 원장)	
10:00~10:50(50')	사 회 **이문규** 교수(인하대)	
	최신 프로세스내 민감데이터 보호기법 본 발표에서는 uMMU(CCS '24) 논문을 중심으로 소프트웨어 취약성 및 부채널 공격으로부터 프로그램의 민감한 데이터를 보호할 수 있는 기술들을 소개합니다.	**이호준** 교수 (성균관대학교)
10:50~11:00(10')	휴식	
11:00~11:50(50')	사 회 **이문규** 교수(인하대)	
	최신 오디오 딥페이크 탐지 기술 ACM CCS 2024에 발표된 Trident of Poseidon을 중심으로, 최근 Audio Deepfake 탐지 기술을 소개합니다	**정수환** 교수 (숭실대학교)
11:50~13:00(70')	중 식	
13:00~13:50(50')	사 회 **권현수** 교수(인하대)	
	시스템 프로그래밍 언어의 메모리 및 타입 취약점 탐지를 위해 개발된 Sanitizer 기술 소개 본 발표에서는 C/C++ 환경에서 발생하는 Custom Memory Allocator 관련 메모리 취약점을 탐지할 수 있는 CMASan (S&P 2024) 및 타입 취약점을 아주 적은 오버헤드로 정확히 탐지할 수 있는 Type++ (NDSS 2025), 그리고 메모리 안전 언어로 알려져 있는 RUST 언어에서 발생할 수 있는 메모리 취약점을 효율적으로 탐지할 수 있는 ERASan (S&P 2025)를 소개합니다.	**전유석** 교수 (고려대학교)
13:50~14:00(10')	휴식	
14:00~14:50(50')	사 회 **권현수** 교수(인하대)	
	Stealing Neural Networks through SW-based power side-channel 이 강연에서는 신경망을 대상으로 한 부채널 공격을 소개합니다. 이후 부채널 공격에 대한 최신 방어 메커니즘들을 살펴보고, SW 기반 전력 부채널 공격이 방어 메커니즘을 어떻게 깰 수 있는지 설명하며, 부채널 공격을 완화시키는 전략에 대해서 논의합니다.	**허준범** 교수 (고려대학교)
14:50~15:00(10')	휴식	
15:00~15:50(50')	사 회 **이용우** 교수(인하대)	
	TLS의 양자내성암호 전환을 위한 효율적인 PQC키 전달 기술 양자내성암호 표준화 동향 및 TLS의 양자내성암호 전환 연구 현황을 소개하고, WWW 2025에서 발표 예정인 ExpressPQDelivery를 중심으로, 효율적인 양자내성암호(PQC) 키 전달 기술을 소개합니다.	**서승현** 교수 (한양대학교)
15:50~16:00(10')	휴식	
16:00~17:00(60')	사 회 **이용우** 교수(인하대)	
	Neural Network Inference over Encrypted Data with High Performance or Accuracy 원격 인공지능 서비스의 확산으로 신경망 추론 연산의 프라이버시 보호가 중요한 과제가 되면서, 동형암호(HE) 기반 PPNNI 연구가 활발히 진행되고 있습니다. 최근에는 신경망 레이어를 산술과 비산술 타입으로 구분해 각각 다른 HE 체계를 적용하는 다종 체계 방식이 주목받고 있지만, 기존 연구들은 기계적인 체계 적용으로 인해 성능 저하 문제가 있었습니다. 본 발표에서는 이를 해결하기 위해 개발한 LOHEN(USENIX Security 2025)을 통해 미세한 정확도 하락을 허용하는 대신 성능을 향상시키고, 레이어 타입을 세분화해 최적의 암호문 구성을 선택함으로써 성능 최적화를 달성한 결과를 소개합니다.	**백윤흥** 교수 (서울대학교)

kips 한국정보처리학회 Korea Information Processing Society 문의처 조환희 사원 02-2077-1414(내선5) chh@kips.or.kr