한국정보보호학회
Korea Institute of Information Security & Cryptology

2025년 한국정보보호학회 동계학술대회

CISC-W'25

Conference on Information Security and Cryptography Winter 2025

2025년 11월 27일(목)~28일(금)

곤지암리조트

주최·주관 한국정보보호학회 Korea Institute of Information Security & Cryptology

후원 국가정보원 NATIONAL INTELLIGENCE SERVICE, 과학기술정보통신부, 행정안전부, KISA 한국인터넷진흥원, ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute, NSR 국가보안기술연구소 National Security Research Institute, KiSTi 한국과학기술정보연구원 Korea Institute of Science and Technology Information www.kisti.re.kr

위원회

학술대회장

한국정보보호학회 회장 박영호 (세종사이버대학교)

조직위원회

- 조직위원장: 하재철 (호서대학교)
- 조직위원: 오진영 (한국인터넷진흥원), 김정녀 (한국전자통신연구원), 한대완 (국가보안기술연구소), 송중석 (한국과학기술정보연구원), 김호원 (부산대학교)

운영위원회

- 운영위원장: 허준범 (고려대학교), 권현수 (인하대학교)
- 운영위원: 구동영 (한성대학교), 남기효 (유니스소프트), 노희준 (인하대학교), 박승현 (한성대학교), 박찬일 (국방과학연구소), 백건대 (한국보안인증), 신영주 (고려대학교), 이윤호 (서울과학기술대학교), 전유석 (고려대학교), 한창희 (서울과학기술대학교)

프로그램 위원회

- 프로그램위원장: 최대선 (숭실대학교), 조효진 (연세대학교)
- 프로그램위원: 강동호 (한국전자통신연구원), 강민석 (한국과학기술원), 곽병일 (고려대학교), 곽 진 (아주대학교), 구본욱 (국가보안기술연구소), 구형준 (성균관대학교), 권동현 (부산대학교), 권태경 (연세대학교), 권태웅 (한국과학기술정보연구원), 김도훈 (경기대학교), 김동우 (동국대학교), 김득훈 (아주대학교), 김범현 (한양대학교), 김성욱 (서울여자대학교), 김수현 (순천향대학교), 김종길 (이화여자대학교), 김종성 (국민대학교), 김진우 (광운대학교), 김태성 (충북대학교), 김현일 (조선대학교), 김형식 (성균관대학교), 김형종 (서울여자대학교), 김환국 (국민대학교), 김효승 (한림대학교), 김휘강 (고려대학교), 김희석 (고려대학교), 노희준 (인하대학교), 도경화 (서강대학교), 류권상 (국립공주대학교), 민병길 (국가보안기술연구소), 박기웅 (세종대학교), 박승현 (한성대학교), 박정수 (강남대학교), 박종근 (한국전자통신연구원), 박종환 (상명대학교), 박철준 (경희대학교), 변진욱 (평택대학교), 서대희 (상명대학교), 서민혜 (덕성여자대학교), 서석충 (국민대학교), 서승현 (한양대학교), 서정택 (가천대학교), 서지원 (단국대학교), 서화정 (한성대학교), 성하영 (한국과학기술정보연구원), 송도경 (연세대학교), 신 욱 (국가보안기술연구소), 양대헌 (이화여자대학교), 오주형 (한국인터넷진흥원), 우사이먼성일 (성균관대학교), 유일선 (국민대학교), 유지현 (광운대학교), 윤명근 (국민대학교), 윤인수 (한국과학기술원), 윤종희 (영남대학교), 윤주범 (세종대학교), 윤택영 (단국대학교), 이경률 (국립목포대학교), 이광수 (세종대학교), 이덕규 (서원대학교), 이만희 (한남대학교), 이문규 (인하대학교), 이병영 (서울대학교), 이석준 (가천대학교), 이선우 (서울여자대학교), 이세영 (강원대학교), 이윤경 (한국전자통신연구원), 이윤호 (서울과학기술대학교), 이일구 (성신여자대학교), 이종혁 (세종대학교), 이 준 (한국과학기술정보연구원), 이창훈 (서울과학기술대학교), 이태진 (가천대학교), 이현우 (한국에너지공과대학교), 임송빈 (한국인터넷진흥원), 임을규 (한양대학교), 임재덕 (한국전자통신연구원), 임준형 (한국인터넷진흥원), 장대희 (경희대학교), 장진수 (충남대학교), 장항배 (중앙대학교), 전상훈 (국민대학교), 전유석 (고려대학교), 정성훈 (숙명여자대학교), 정익래 (고려대학교), 조남수 (단국대학교), 조해현 (숭실대학교), 주경호 (숭실대학교), 지승구 (한국인터넷진흥원), 최선오 (전북대학교), 최원석 (고려대학교), 최윤호 (부산대학교), 한승훈 (숭실대학교), 홍득조 (전북대학교), 홍준호 (성신여자대학교), 황성재 (성균관대학교)

(최)우수논문

번호	상장	논문번호	논문명	저자
1	과기부 장관상	110	Pig Butchering 사기의 체계적 공격 패턴 분석: ChainAbuse 신고 데이터 기반 실증적 연구	류나연, 이세영(강원대학교)
2	행안부 장관상	81	ICL 기반 백도어 공격을 통한 LLM 추론 과정 안전성 평가	박성규, 박소희, 이원호, 최대선(숭실대학교)
3	학회 최우수논문상	214	CTI 보고서 분석 정확도 향상을 위한 Vision-Language 모델 프롬프팅 전략 연구	김서연, 이새움, 최슬기, 김태현, 오동환, 임준형, 김태은(한국인터넷진흥원)
4	학회 최우수논문상	111	RLHF의 한계 보완을 위한 RAG 기반 Lifelong 가드레일	김현서(호서대학교), 한태현, 이태진(가천대학교)
5	학회 최우수논문상	139	핵심 기반 시설 대상의 공격 시나리오 생성을 위한 MITRE CTI 통합 및 자동화 파이프라인 설계	노성현, 김태성(충북대학교)
6	KISA 원장상	233	XPC 및 IOKit 기반 macOS 공격 표면 식별 자동화	이동하, 강민주, 한규상, 박정우, 전승호(가천대학교)
7	KISA 원장상	87	에이전틱 AI 기반 자율형 데이터 유출 방지	조항범, 오주엽, 박찬민, 최영락, 손현기, 윤명근(국민대학교)
8	KISA 원장상	126	SPADE-XR: XR 환경에서의 공간 데이터 권한 불일치 탐지 및 분석 프레임워크	주효중, 이승수(인천대학교)
9	ETRI 원장상	183	Hardening Control-Flow Integrity via Program Context Concretization	변현수(서울과학기술대학교), 권용휘(메릴랜드대학교), 이창훈(서울과학기술대학교)
10	ETRI 원장상	212	언러닝 위장 공격: 머신 언러닝에 대한 새로운 공격 벡터	박선혜, 김형식(성균관대학교)
11	ETRI 원장상	227	퍼징을 위한 Windows 커널 드라이버 정적 분석	임미래, 오세환, 조해현(숭실대학교)
12	NSR 소장상	246	다중 도메인 접근법을 이용한 전자기파 기반 이상 탐지 연구	박수진, 배대현, 이인섭, 김희석(고려대학교), 홍석희(컨텍)
13	NSR 소장상	273	대규모 언어 모델 기반 코딩 에이전트의 보안성 분석 및 공격 시나리오 실증 연구	이은규, 김동현, 김원영, 윤인수(한국과학기술원)
14	NSR 소장상	321	시스템 자원 분석을 통한 PQC 알고리즘 적합성 평가 및 추천 프레임워크	송민호, 엄시우, 윤세영, 서화정(한성대학교)
15	KISTI 원장상	325	JPEG 압축에 강건한 이미지 백도어 삽입 기법 제안	이성은, 지일환, 이주현, 서정택(가천대학교)
16	KISTI 원장상	328	디지털 포렌식 관점에서의 Threads 사용자 행위 분석	김강민, 변현수, 조민정, 김역, 손기욱, 이창훈(서울과학기술대학교)
17	KISTI 원장상	24	STFT-ResNet 기반 하드웨어 트로이목마 탐지 및 XAI 분석	오충연, 한동국(국민대학교)
18	학회 우수논문상	247	국내 LTE/IMS 환경에서의 SMS 평문전송 및 도청 위험 실증 연구	이동원, 변민주(경희대학교), 최현영(엔에스원소프트), 박철준(경희대학교)
19	학회 우수논문상	265	누적 분산 알고리즘을 통한 부채널 누수 평가 최적화	신원근, 전승현, 김희석(고려대학교)
20	학회 우수논문상	294	네트워크 트래픽 기반 TTP 식별 및 라벨링 연구 동향	박한솔, 백의준, 이준(한국과학기술정보연구원)
21	학회 우수논문상	33	양자 시대로의 전환에서 전자서명의 무결성 보장	이동욱, 김재윤, 조남수, 윤택영(단국대학교)
22	학회 우수논문상	44	Matter 프로토콜 취약점 분석 및 보안 연구	성준우(영남이공대학교), 한승훈(숭실대학교)
23	학회 우수논문상	62	MITRE ATT&CK-D3FEND 지식 그래프 기반의 위협 대응 우선순위 모델	한희수, 최상훈, 박기웅(세종대학교)

번호	상장	논문번호	논문명	저자
24	학회 우수논문상	63	HWTypeSan: ARM 포인터 인증 기반의 효율적인 타입 안전성 위반 취약점 탐지 도구	최민성, 전유석(고려대학교)
25	학회 우수논문상	70	Adversarial Attacks on Autonomous Systems: Emerging Threats	Thi-Thu-Huong Le, Andro Aprila Adiputra, 장현진, 김호원(부산대학교)
26	학회 우수논문상	74	FIDS: A Fake MQTT-Network Traffic Intrusion Detection System via Hybrid Semantic-Lexical Meta-Classification	Abhishek Chaudhary, 김병찬, 최선오(전북대학교)
27	학회 우수논문상	82	인터넷 연결 자산 및 위협 검색 기반 선박 장비 원격 관리 인터페이스 취약점 분석	이진성, 나사랑, 김대운, 임준형(한국인터넷진흥원)
28	학회 우수논문상	16	Negative Dentry를 이용한 Covert Channel 구현	윤홍국, 김호동, 허준범(고려대학교)
29	학회 우수논문상	19	군집 주행 환경에서의 동기식 가명 교체 방법	이준택, 김찬민, 권민희(한국자동차연구원)
30	학회 우수논문상	28	리눅스 및 ESXi 클라우드 호스트 환경에서의 랜섬웨어 행위 분석	최진우, 김진우(광운대학교)
31	학회 우수논문상	36	NFT 이미지 가용성의 붕괴: 접근 불가능한 Web2 서버 내 NFT 자산에 대한 비교 연구	김건희, 김도연, 박제만(경희대학교)
32	학회 우수논문상	43	프레임 기반 딥페이크 탐지를 위한 CNN-UniFormer 하이브리드 모델 연구	윤상원, 고강민, 진예찬, 최석환(연세대학교)
33	학회 우수논문상	137	CLOVA Note API 기반 음성 포렌식 및 발화 분석 연구	최종윤, 신민석, 김한결, 위다빈, 박명서(한성대학교)
34	학회 우수논문상	239	AES-GCM Pre-computation 기법을 통한 ROS 2 암호화 통신 성능 개선	나보림, 유진호, 조효진(연세대학교)

프로그램 일정표

2025년 11월 27일 (목)

	구두트랙1	구두트랙2	구두트랙3	구두트랙4	구두트랙5	구두트랙6	구두트랙7	구두트랙8	포스터세션
시간/장소	컨퍼런스 L1 (B1F)	컨퍼런스 L2 (B1F)	컨퍼런스 L3 (B1F)	컨퍼런스 L4 (B1F)	컨퍼런스 L5 (B1F)	컨퍼런스 L6 (B2F)	컨퍼런스 L7 (B2F)	컨퍼런스 L8 (B2F)	컨벤션홀 (B2F)
10:00~11:00	참가자 등록 그랜드볼룸 앞 (E/W빌리지 B2F)								
11:00~12:00	좌장: 김범현 (한양대)	좌장: 류권상 (국립공주대)	좌장: 송현민 (단국대)	좌장: 서화정 (한성대)	좌장: 석병진 (한성대)	좌장: 조성민 (ETRI)	좌장: 권태웅 (KISTI)	좌장: 조남수 (단국대)	좌장: 주경호 (숭실대)
	(1-1) 해킹과 취약점 분석 I	(1-2) 인공지능 보안 I	(1-3) 인공지능 보안 II	(1-4) 부채널 보안 I	(1-5) 융합 보안 I	(1-6) 양자보안 I	(1-7) 네트워크 보안 I	(1-8) 암호이론과 구현 I	Poster Session I
12:00~13:00	중식 카페테리아 (스키하우스 2F)								
13:00~14:00	좌장: 주경호 (숭실대)	좌장: 석병진 (한성대)	좌장: 이현우 (KENTECH)	좌장:이승광 (단국대)	좌장: 김득훈 (아주대)	좌장: 서화정 (한성대)	좌장: 박철준 (경희대)	좌장: 윤택영 (단국대)	좌장:김효승 (한림대)
	(2-1) 해킹과 취약점 분석 II	(2-2) 인공지능 보안 III	(2-3) 인공지능 보안 IV	(2-4) 부채널 보안 II	(2-5) 융합 보안 II	(2-6) 양자보안 II	(2-7) 네트워크 보안 II	(2-8) 암호이론과 구현 II	Poster Session II
14:00~14:10	휴식								
14:10~15:10	좌장: 박기웅 (세종대)	좌장: 이태진 (가천대)	좌장: 김현일 (조선대)	좌장:서지원 (단국대)	좌장: 이덕규 (서원대)	좌장: 이창민 (고려대)	좌장: 박정수 (강남대)	좌장: 이문규 (인하대)	좌장: 이윤호 (서울과기대)
	(3-1) 해킹과 취약점 분석 III	(3-2) 인공지능 보안 V	(3-3) 인공지능 보안 VI	(3-4) SW/시스템 보안 I	(3-5) 융합 보안 III	(3-6) 양자보안 III	(3-7) 네트워크 보안 III	(3-8) 암호이론과 구현 III	Poster Session III
15:10~15:20	휴식								
15:20~15:50 (30분)	신진연구자 소개 세션(좌장: 숭실대 최대선, 연세대 조효진) 그랜드볼룸 (E/W빌리지 B2F) 신진연구자: 한성대 석병진, 대검찰청 김기윤, 숭실대 주경호, 고려대 이창민, 가천대 전승호, ETRI 조성민, KISA 강상용, 한양대에리카 김범현								
15:50~16:00	휴식								
16:00~16:50 (50분)	개회식 그랜드볼룸 (E/W빌리지 B2F)								
	사회: 운영위원장 허준범(고려대), 권현수(인하대) 국민의례 내빈소개 개회사 : 한국정보보호학회 회장 박영호 행사보고(프로그램위원장 최대선(숭실대), 조효진(연세대)) (최)우수논문 시상 경품추첨								
16:50~17:00	휴식								
17:00~18:00	정기총회 그랜드볼룸 (E/W빌리지 B2F)								
19:00~	만찬 학생 : 그랜드볼룸 (E/W 빌리지 B2F), 일반 : 미라시아 (빌리지센터 1F)								

프로그램 일정표

2025년 11월 28일 (금)

	구두트랙1	구두트랙2	구두트랙3	구두트랙4	구두트랙5	구두트랙6	구두트랙7
시간/장소	컨퍼런스 L1 (B1F)	컨퍼런스 L2 (B1F)	컨퍼런스 L3 (B1F)	컨퍼런스 L4 (B1F)	컨퍼런스 L5 (B1F)	컨퍼런스 M7 (1F)	컨퍼런스 M8 (1F)
08:00~09:00	조식 카페테리아 (스키하우스 2F)						
09:00~09:20	참가자 등록 컨퍼런스 L1 옆 (E/W빌리지 B1F)						
09:20~10:20	좌장: 김기윤 (대검찰청)	좌장: 류권상 (국립공주대)	좌장: 강상용 (KISA)	좌장: 조효진 (연세대)	좌장: 김득훈 (아주대)	좌장: 전승호 (가천대)	좌장: 구본욱 (국보연)
	(4-1) 디지털 포렌식 I	(4-2) 인공지능 보안 VII	(4-3) 인공지능 보안 VIII	(4-4) SW/시스템 보안 II	(4-5) 융합보안IV	(4-6) 블록체인 보안	(4-7) 암호이론과 구현 IV
10:20-10:30	휴식						
10:30-11:30	좌장: 김종성 (국민대)	좌장: 윤주범 (세종대)	좌장: 서승현 (한양대)	좌장: 전승호 (가천대)	좌장: 박철준 (경희대)	좌장: 이만희 (한남대)	좌장: 조효진 (연세대)
	(5-1) 디지털 포렌식 II	(5-2) 인공지능 보안 IX	(5-3) 인공지능 보안 X	(5-4) SW/시스템 보안 III	(5-5) IoT/CPS 보안 I	(5-6) 공급망 보안 I	(5-7) 산업보안
11:30-11:40	휴식						
11:40-12:40	좌장: 홍준호 (성신여대)	좌장:서승현 (한양대)	좌장: 김기윤 (대검찰청)	좌장: 윤주범 (세종대)	좌장: 임재덕 (ETRI)	좌장: 최대선 (숭실대)	좌장: 류권상 (국립공주대)
	(6-1) 정보보호 정책, 법, 제도	(6-2) 이동통신 보안	(6-3) 모바일 보안	(6-4) SW/시스템 보안 IV	(6-5) IoT/CPS 보안 II	(6-6) 공급망 보안 II	(6-7) 개인정보보호
12:40-14:00	중식 학생: 카페테리아 (스키하우스 2F), 일반: 미라시아 (빌리지센터 1F)						

※ 한국정보보호학회 2025년 동계학술대회에서 발표되는 모든 논문(구두발표, 포스터발표)은 2025년 동계학술대회에 게재되는 일반 논문입니다.

구두발표 세션

2025년 11월 27일(목)

세션	논문번호	논문제목(저자)
11:00~12:00 (1-1) 해킹과 취약점 분석 I 좌장: 김범현 (한양대)	227	퍼징을 위한 Windows 커널 드라이버 정적 분석 임미래, 오세환, 조해현(숭실대학교)
	233	XPC 및 IOKit 기반 macOS 공격 표면 식별 자동화 이동하, 강민주, 한규상, 박정우, 전승호(가천대학교)
	28	리눅스 및 ESXi 클라우드 호스트 환경에서의 랜섬웨어 행위 분석 최진우, 김진우(광운대학교)
	60	문법 기반 퍼징을 통한 WASI 런타임의 권한 취약점 탐지 이준호, 박요한, 김진우(광운대학교)
11:00~12:00 (1-2) 인공지능 보안 I 좌장: 류권상 (국립공주대)	81	ICL 기반 백도어 공격을 통한 LLM 추론 과정 안전성 평가 박성규, 박소희, 이원호, 최대선(숭실대학교)
	100	이미지 생성 모델에서의 Concept embedding layer를 활용한 유해 콘텐츠 생성 완화 기법 오세원, 박소희, 김승민, 최대선(숭실대학교)
	212	언러닝 위장 공격: 머신 언러닝에 대한 새로운 공격 벡터 박선혜, 김형식(성균관대학교)
	214	CTI 보고서 분석 정확도 향상을 위한 Vision-Language 모델 프롬프팅 전략 연구 김서연, 이새움, 최슬기, 김태현, 오동환, 임준형, 김태은(한국인터넷진흥원)
11:00~12:00 (1-3) 인공지능 보안 II 좌장: 송현민 (단국대)	273	대규모 언어 모델 기반 코딩 에이전트의 보안성 분석 및 공격 시나리오 실증 연구 이은규, 김동현, 김원영, 윤인수(한국과학기술원)
	325	JPEG 압축에 강건한 이미지 백도어 삽입 기법 제안 이성은, 지일환, 이주현, 서정택(가천대학교)
	24	STFT-ResNet 기반 하드웨어 트로이목마 탐지 및 XAI 분석 오충연, 한동국(국민대학교)
	108	다중 홉 추론형 의료 질의응답 AI 에이전트 이채린, 서채원, 최대선(숭실대학교)
11:00~12:00 (1-4) 부채널 보안 I 좌장: 서화정 (한성대)	265	누적 분산 알고리즘을 통한 부채널 누수 평가 최적화 신원근, 전승현, 김희석(고려대학교)
	234	픽스슬라이싱 기법을 활용한 새로운 부채널 공격 대응 기법 김동현, 신한범, 김희석(고려대학교), 홍석희(컨텍)
	57	고사양 장비에 대한 교차 장비 딥러닝 프로파일링 부채널 분석 노혜빈, 한동국(국민대학교)
	230	SEV-Step 프레임워크의 재현성에 대한 실험적 검증 오승준, 김태훈, 신영주(고려대학교)

구두발표 세션

2025년 11월 27일(목)		
세션	논문번호	논문제목(저자)
11:00~12:00 (1-5) 융합 보안 I 좌장: 석병진 (한성대)	70	Adversarial Attacks on Autonomous Systems: Emerging Threats Thi-Thu-Huong Le, Andro Aprila Adiputra, 장현진, 김호원(부산대학교)
	19	군집 주행 환경에서의 동기식 가명 교체 방법 이준택, 김찬민, 권민희(한국자동차연구원)
	42	Social VR Administrator: 소셜 VR내 괴롭힘 방지를 위한 상황 인지형 모델 에이전트 디자인 이준희, 김민석(광운대학교), 허환조, 우승원(ETRI), 김진우(광운대학교)
	88	운항 선박 환경에서의 자산 가시성 제공을 위한 RAG 기반 자동 식별 방법 김진강, 나사랑, 박성민, 임준형(한국인터넷진흥원)
11:00~12:00 (1-6) 양자보안 I 좌장: 조성민 (ETRI)	321	시스템 자원 분석을 통한 PQC 알고리즘 적합성 평가 및 추천 프레임워크 송민호, 엄시우, 윤세영, 서화정(한성대학교)
	253	KpqC 격자 기반 암호의 임베디드 환경 성능 분석 및 실사용 가능성 연구 박경빈, 김현주(국립공주대학교), 임우상(대구경북과학기술원), 강찬구(라온컨버전스), 서창호(국립공주대학교)
	322	NTT 기반 쇤하게-슈트라센 알고리즘 정수 곱셈의 양자 회로 설계 신다윗, 조재한, 김호원(부산대학교)
	103	GPU 기반 SMAUG-T 병렬 최적화 연구 고주희, 최준혁, 김동천, 서석충(국민대학교)
11:00~12:00 (1-7) 네트워크 보안 I 좌장: 권태웅 (KISTI)	216	LoRaWAN에 대한 네트워크 보안 취약점 및 대응 방안 분석 이광용, 김윤성, 이혜강, 하재철(호서대학교)
	294	네트워크 트래픽 기반 TTP 식별 및 라벨링 연구 동향 박한솔, 백의준, 이준(한국과학기술정보연구원)
	178	평균 기반 유사도 보정기법을 이용한 암호화 트래픽 분류 향상 연구 김찬형, 윤종희(영남대학교)
	50	저궤도 위성 네트워크의 안전한 클러스터링을 위한 보안 기술 연구 명재민, 서대희(상명대학교)
11:00~12:00 (1-8) 암호이론과 구현 I 좌장: 조남수 (단국대)	31	결합 안전성이 등장하기 이전 고차 AES 마스킹에 대한 부채널 분석 잔여 취약점 공격 및 해결 방안 안현준, 한동국(국민대학교)
	228	SQIsign의 고정 정밀도 정수 산술 구현 김원, 이정환, 김현학, 이창민(고려대학교)
	215	축소 라운드 LBC-IoT 블록암호에 대한 선형 분석 권혁태, 박준영, 송원우, 김남일, 백승준, 김종성(국민대학교)
	254	이더리움 EOA 탈취 공격에 대한 저항성 증명 연구 손혜은, 김효승(한림대학교)

구두발표 세션

2025년 11월 27일(목)

세션	논문번호	논문제목(저자)
13:00~14:00 (2-1) 해킹과 취약점 분석 II 좌장: 주경호 (숭실대)	196	문법 기반 적응형 퍼징을 이용한 webOS Luna API의 취약점 탐지 박재유, 홍현지, 박세기, 조혜진(LG전자)
	159	Android 환경에서의 비밀번호 관리 애플리케이션 PasswordSafe와 NordPass 복호화 및 보안성 분석 김태환, 안현종, 김종성(국민대학교)
	123	네트워크형 PoC 공격 코드의 패키지 사용 패턴과 방어 시사점 이재희 ,박준형, 안효범(국립공주대학교)
	310	패스워드 크래킹 고도화 기술 분석 김영진, 김하민, 조민정, 김역, 손기욱, 이창훈(서울과학기술대학교)
13:00~14:00 (2-2) 인공지능 보안 III 좌장: 석병진 (한성대)	111	RLHF의 한계 보완을 위한 RAG 기반 Lifelong 가드레일 김현서(호서대학교), 한태현, 이태진(가천대학교)
	150	MCP Argus: 합성 MCP 서버 공격 완화를 위한 선제적 미들웨어 김아인, 이승수(인천대학교)
	74	FIDS: A Fake MQTT-Network Traffic Intrusion Detection System via Hybrid Semantic-Lexical Meta-Classification Abhishek Chaudhary, 김병찬, 최선오(전북대학교)
	107	연합학습에서의 다중 참조 기반 포이즈닝 공격 탐지 류상범, 박소희, 이지수, 최대선(숭실대학교)
13:00~14:00 (2-3) 인공지능 보안 IV 좌장: 이현우 (KENTECH)	290	Prefix Tuning 기반 대규모 언어모델 소유권 검증 기법 유경빈, 김형식(성균관대학교)
	313	RelationMesh: 설명 가능한 비지도 이상탐지 모델 김병록, 이현우(한국에너지공과대학교)
	32	그래프를 활용한 오픈 데이터 & LLM 벤치마크 오염 탐지 연구 동향 김규영, 최나영, 최대선(숭실대학교)
	43	프레임 기반 딥페이크 탐지를 위한 CNN-UniFormer 하이브리드 모델 연구 윤상원, 고강민, 진예찬, 최석환(연세대학교)
13:00~14:00 (2-4) 부채널 보안 II 좌장:이승광 (단국대)	101	A Study on Evaluation Criteria for Second-Order Fault Injection Resistance 조홍래, 한동국(국민대학교)
	164	e-Cryptex 기반 EM 부채널 방어 보안 프레임워크 설계 김효찬, 한미란, 이중희(고려대학교)
	211	캐시 주소 무작위화를 위한 트위커블 블록암호 SCARF에 대한 부채널 공격 강동우, 이인훈, 김희석(고려대학교), 홍석희(컨텍)
	246	다중 도메인 접근법을 이용한 전자기파 기반 이상 탐지 연구 박수진, 배대현, 이인섭, 김희석(고려대학교), 홍석희(컨텍)

구두발표 세션

2025년 11월 27일(목)

세션	논문번호	논문제목(저자)
13:00~14:00 (2-5) 융합 보안 II 좌장: 김득훈 (아주대)	129	VANET 환경에서 동적 그룹 관리를 위한 스마트 계약 기반 멤버 인증에 관한 연구 조현아, 박유란, 김수현, 이임영(순천향대학교)
	286	차량용 IDS를 위한 이미지 인식 딥러닝 기반의 공격 탐지 기법 이재우, 최원석(고려대학교)
	307	OPC UA 프로토콜 대상 구현체별 Password Downgrade 공격 검증 박미리, 이주현, 서정택(가천대학교)
	320	산업제어시스템 운영환경을 반영한 특징 추출 기법 연구 및 이상탐지 유효성 검증 최현서, 지일환, 이주현, 서정택(가천대학교)
13:00~14:00 (2-6) 양자보안 II 좌장: 서화정 (한성대)	210	PQC 하이브리드 인증서 밴치마킹 연구 이여녕, 김제인, 서승현(한양대학교)
	219	코드기반암호에 대한 양자 공격 비용 분석 장경배, 서화정(한성대학교)
	223	FTQC 환경을 고려한 T-Depth 효율화 HIGHT 양자 회로 LisaBabu 가산기 기반 접근법 안재만, 오진섭, 김호영, 최순욱, 최두호(고려대학교)
	326	QSF 기반 하이브리드 KpqC KEM에 대한 Cortex-M4 환경에서의 성능 평가 장지훈, 강태훈, 이명훈(고려대학교), 석병진(한성대학교), 김수리(성신여자대학교), 홍석희(컨텍), 이상진(고려대학교)
13:00~14:00 (2-7) 네트워크 보안 II 좌장: 박철준 (경희대)	58	HD-NIDSBench: 고차원 컴퓨팅을 활용한 효율적인 침입탐지 시스템에 대한 벤치마킹 프레임워크 강윤의(KENTECH), 김지승, 김예승(DGIST), 김현주, 이현우(KENTECH)
	91	HSJA 기반 기만공격 징후 분석과 NIDS별 쿼리 효율 비교 민동욱, 오윤주, 김도완, 최대선(숭실대학교)
	308	앙상블 기법을 활용한 인공지능 기반 보안관제 탐지 정확도 향상 연구 안도현, 차충일, 성하영(한국과학기술정보연구원)
	275	Athena 기반 SQL-as-Rules 접근법을 활용한 AWS 환경 SSRF 탐지 연구 이은사, 신예은, 윤성원, 임서영, 김경진(성신여자대학교)
13:00~14:00 (2-8) 암호이론과 구현 II 좌장: 윤택영 (단국대)	180	고정키 환경에서의 Alzette 안전성 분석 이명규, 황윤재, 신한범, 김인성, 김선엽(고려대학교), 석병진(한성대학교), 이동재(강원대학교), 홍득조(전북대학교), 성재철(서울시립대학교), 홍석희(컨텍)
	194	ARIA 블록암호 기반 HCTR2 운용모드의 성능 분석 및 최적화 엄시우, 송민호, 윤세영, 서화정(한성대학교)
	213	SKINNY-64-64에 대한 주성분 분석 기반 Integral Cryptanalysis 황윤재, 이명규, 김인성, 신한범, 김선엽(고려대학교), 석병진(한성대학교), 홍석희(컨텍), 이상진(고려대학교)
	177	32-bit ARM Cortex-M3 상에서의 CHAM-64/128 병렬 암호화 구현 김은석(전북대학교), 신명수(에너자이), 홍득조(전북대학교)

2025년 11월 27일(목)

세션	논문번호	논문제목(저자)
14:10~15:10 (3-1) 해킹과 취약점 분석 III 좌장: 박기웅 (세종대)	192	오픈소스 클라우드 보안 도구 비교 분석 및 통합 활용전략 연구 김도영, 공나영, 최상훈, 박기웅(세종대학교)
	22	목표 지향 프로토콜 취약점 탐지 도구 설계 엄재은, 전유석(고려대학교)
	232	USB를 사용한 ADB 통신에서 개인정보 유출 가능성 분석 강창협, 김민교, 김민수(국립목포대학교)
	329	저가형 상용 드론의 하드웨어 수준 취약점 분석 황철민, 이승준(bornlake)
14:10~15:10 (3-2) 인공지능 보안 V 좌장: 이태진 (가천대)	67	Dynamic Class Awareness: Towards Sparse Taxonomy Learning 아궁, 장현진, 레티 투 흐엉, 김호원(부산대학교)
	72	스타일 변형 이미지 탐지를 위한 CLIP 유사도 임계값 연구 박건, 백성실, 신수홍, 남시영, 우재영, 김혜영(홍익대학교)
	90	MCP Host 행위 모니터링을 통한 Agentic AI 시스템의 보안 가시성 확보 및 위협 탐지 프레임워크 양승원(건국대학교), 한고원(부산대학교), 최준혁(고려대학교), 성호건(연세대학교), 김정택(가천대학교)
	144	다중 AI 에이전트 시스템의 보안 위협 분석 신수진(국립부경대학교), 노시완(동의대학교), 신상욱(국립부경대학교)
14:10~15:10 (3-3) 인공지능 보안 VI 좌장: 김현일 (조선대)	115	적대적 공격을 통한 오픈소스 AI 모델의 강건성 분석 조수빈, 김하경, 김송연, 박주현, 석병진(한성대학교)
	127	AI 신뢰원칙 기반 LLM 안전성 평가 방법론 연구 서유민(호서대학교), 한태현, 이태진(가천대학교)
	135	MLP 뉴런에 대한 오류 주입 공격 영향도 분석 김수형, 이상원, 김윤성, 하재철(호서대학교)
	148	Open-RAN 환경 메타학습과 강화 학습 기반 차분 프라이버시 시스템 최적화 차한솔, 김가경, 김종현(세종대학교)
14:10~15:10 (3-4) SW/시스템 보안 I 좌장:서지원 (단국대)	168	이기종 보안 솔루션의 통합 및 연동성 향상을 위한 로그 포맷 자동 식별 시스템 이도현, 오동환, 이새움, 최슬기, 김태현, 김서연, 임준형, 김태은(한국인터넷진흥원)
	199	동적 취약점 분석 결과의 중복 제거 기법 연구 동향 분석 김태호, 권태경(연세대학교)
	237	TSAN--: Remaining Challenges for Debloating Thread Sanitizer 정성윤, 전유석(고려대학교)
	240	랜섬웨어의 암호화 루프 감지 및 분석 김동우, 조해현(숭실대학교)

2025년 11월 27일(목)

세션	논문번호	논문제목(저자)
14:10~15:10 (3-5) 융합 보안 III 좌장: 이덕규 (서원대)	37	End-to-End 자율주행 모델에 대한 적대적 공격 분석 조강모, 주경호(숭실대학교)
	125	제조 공정 및 자율 이동 로봇의 보안 동향 분석 김희찬, 이경민, 손준영(부산대학교)
	133	차량용 인포테이먼트 기반 사용자 행위 추적 김대환, 신민석, 장규영, 안원석, 박명서(한성대학교)
	221	Analysis of Authentication Vulnerabilities and Mitigating Methods in V2G Charging and Payment Systems 가드라 나무라타, 김태우, 김득훈, 곽진(아주대학교)
14:10~15:10 (3-6) 양자보안 III 좌장: 이창민 (고려대)	33	양자 시대로의 전환에서 전자서명의 무결성 보장 이동욱, 김재윤, 조남수, 윤택영(단국대학교)
	99	CRYSTALS-KYBER 대상 단일파형공격 동향 분석 이민정, 유성환, 한동국(국민대학교)
	298	ARM Cortex-M4 상에서의 불완전 NTT를 사용한 SMAUG-T 곱셈 알고리즘 구현 윤성우, 목정현, 박지민, 박소영, 이석준(가천대학교)
	280	양자 취약탐지 프레임워크 적용 및 개선 방향 지찬웅, 서승현(한양대학교)
14:10~15:10 (3-7) 네트워크 보안 III 좌장: 박정수 (강남대)	311	실용적 비복호화 기반 암호화 트래픽 악성 행위 탐지를 위한 Transformer 모델 연구 권태웅, 김태용, 송중석(한국과학기술정보연구원)
	16	Negative Dentry를 이용한 Covert Channel 구현 윤홍국, 김호동, 허준범(고려대학교)
	77	AWS 로그 기반 침해사고 식별 및 대응 자동화 프레임워크 김도연(서울여자대학교), 김수민(성신여자대학교), 조휘정(이화여자대학교), 노태영(KITRI Best of the Best), 안관우(아주대학교), 이유빈(성신여자대학교), 박후린(서울여자대학교)
	182	클라우드 환경에서 eBPF와 LLM을 활용한 APT 탐지 프레임워크 설계 김종섭, 손창민, 김진우(광운대학교)
14:10~15:10 (3-8) 암호이론과 구현 III 좌장: 이문규 (인하대)	83	경량 해시 함수 기반 BSG 구조의 개선 방안 김민규, 김민규, 김종현(세종대학교)
	143	표준 블록 암호 LEA 및 HIGHT의 영지식 증명 효율성 분석 차영훈(한양대학교), 정한힘, 김지혜(국민대학교), 오현옥(한양대학교)
	167	동형암호 알고리즘 구현 적합성 검증 체계 설계 및 분석 김태훈, 차명훈, 손기종(한국인터넷진흥원)
	76	접근제어를 제공하는 트랩도어 기반 KA-PRE 기법 연구 신재정, 김수현, 이임영(순천향대학교)

2025년 11월 28일(금)

세션	논문번호	논문제목(저자)
09:20~10:20 (4-1) 디지털 포렌식 I 좌장: 김기윤 (대검찰청)	328	디지털 포렌식 관점에서의 Threads 사용자 행위 분석 김강민, 변현수, 조민정, 김역, 손기욱, 이창훈(서울과학기술대학교)
	161	카카오톡 메시지 수정 기능의 포렌식 분석 김주미(성균관대학교), 김용진(가천대학교), 김도현(전주대학교), 김기범(성균관대학교)
	175	디지털포렌식 도구의 파일 포맷 파싱 기능 검증: ZIP 포맷을 중심으로 박예원, 정수은, 박정흠(고려대학교)
	137	CLOVA Note API 기반 음성 포렌식 및 발화 분석 연구 최종윤, 신민석, 김한결, 위다빈, 박명서(한성대학교)
09:20~10:20 (4-2) 인공지능 보안 VII 좌장: 류권상 (국립공주대)	195	기업 환경에서 LLM 및 MCP 사용 시 중요정보 유출 차단을 위한 통합 보안 프레임워크 연구 김민서(성공회대학교), 박하은(가천대학교), 이강호(아주대학교), 이시온(세종대학교), 최원혁(성공회대학교), 박경재(에이치엠컴퍼니)
	203	MLOps 환경에서의 데이터 누수 위협 분석을 통한 MLOps 보안 통제 방안 제안 권노경, 김수민(서울여자대학교), 황혜경(세종대학교), 양종호(순천향대학교), 한철규(LG CNS)
	229	PRECOG: Prediction-based defense system for multi-turn attacks 박제호, 최대선(숭실대학교)
	255	강화학습을 이용한 CADO-NFS 다항식 선택 파라미터 최적화 김제빈, 이인섭, 전찬호(고려대학교), 김수리(성신여자대학교), 홍석희(컨텍), 이상진(고려대학교)
09:20~10:20 (4-3) 인공지능 보안 VIII 좌장: 강상용 (KISA)	324	자동화된 Strategy 생성 기반 LLM jailbreaking 고도화 방안 연구 오정민, 한태현, 이태진(가천대학교)
	5	Differentially Private Federated Learning for Clinical Trial Optimization 누룰 하지라 빈티 모하마다 놀, 최윤호(부산대학교)
	39	페르소나 주입과 교차 언어 음차를 이용한 텍스트-이미지 생성 모델의 신규 취약점 분석 서희영, 이세영(강원대학교)
09:20~10:20 (4-4) SW/시스템 보안 II 좌장: 조효진 (연세대)	289	파생 프로젝트 취약점 탐지를 위한 다중 시드 퓰 퍼저 전세옥, 윤상권, 최광훈(전남대학교), 김석휘, 김건오(케이사인)
	26	LLM 기반 코드 생성 도구의 정보 부족 유래 취약점 완화를 위한 축약 컨텍스트 구성 디자인 제안 이서현, 전유석(고려대학교)
	30	악성코드 난독화 성능 평가에 대한 연구: 데이터 난독화부터 LLM 기반 난독화까지 최준우, 김태용, 박수연, 유예찬, 최석환(연세대학교)
	186	WebAssembly와 Proxy를 악용하는 악성 Chrome 확장프로그램 연구 문영민, 홍민혁, 박제만(경희대학교)

구두발표 세션

2025년 11월 28일(금)		
세션	논문번호	논문제목(저자)
09:20~10:20 (4-5) 융합보안IV 좌장: 김득훈 (아주대)	131	전기 자동차 충전 시스템을 위한 효율적인 인증 기법 연구 이승빈, 이수왕, 김지윤(경상국립대학교)
	239	AES-GCM Pre-computation 기법을 통한 ROS 2 암호화 통신 성능 개선 나보림, 유진호, 조효진(연세대학교)
	272	K-RMF 기반 무인항공기 보안통제항목 조정 초기 단계 적용 연구 이서희, 송유래, 김득훈, 곽진(아주대학교)
	126	SPADE-XR: XR 환경에서의 공간 데이터 권한 불일치 탐지 및 분석 프레임워크 주효중, 이승수(인천대학교)
09:20~10:20 (4-6) 블록체인 보안 좌장: 전승호 (가천대)	110	Pig Butchering 사기의 체계적 공격 패턴 분석: ChainAbuse 신고 데이터 기반 실증적 연구 류나연, 이세영(강원대학교)
	36	NFT 이미지 가용성의 붕괴: 접근 불가능한 Web2 서버 내 NFT 자산에 대한 비교 연구 김건희, 김도연, 박제만(경희대학교)
	287	블록체인 기반 합성데이터 신뢰 및 투명성 보장 프레임워크 정은혜, 이경현(국립부경대학교)
	4	신뢰성 제공을 위한 스테이블코인의 법정화폐 상환 체계 강환철(금융결제원)
09:20~10:20 (4-7) 암호이론과 구현 IV 좌장: 구본욱 (국보연)	66	1:n 환경을 위한 Designated Verifier Signature에 대한 연구 윤성철, 김수현, 이임영(순천향대학교)
	188	모듈러 곱셈의 기계적 검증: EasyCrypt를 통한 형식 검증 방법론 지용현, 서석충(국민대학교)
	124	형태보존암호 FF1의 고속화 및 경량화 기법 연구 백승훈, 김수현(순천향대학교)
	248	A Blockchain-based ESG Certification Framework for Privacy and Verifiable Sustainability Cho Nwe Zin Latt, 이경현(부경대학교)

2025년 11월 28일(금)

세션	논문번호	논문제목(저자)
10:30-11:30 (5-1) 디지털 포렌식 II 좌장: 김종성 (국민대)	189	안드로이드용 악성코드 보호 기법 분석 및 역분석 도구 설계 및 구현 남태호(국가보안기술연구소)
	121	오픈소스 기반의 Yurei 랜섬웨어에 대한 동작 분석 및 연관성 식별 연구 김한결, 위다빈, 최종윤, 신민석, 박명서(한성대학교)
	134	AI 생성 콘텐츠 시대의 저작권 포렌식 기술 동향 분석 장규영, 김동인, 박명서(한성대학교)
	238	LLM 기반 악성코드 동적 분석 자동화 시스템 설계 이형규(국가보안기술연구소)
10:30-11:30 (5-2) 인공지능 보안 IX 좌장: 윤주범 (세종대)	95	LLM 탈옥 탐지기의 의미 기반 평가를 위한 핵심 질의 추출 접근법 김하준, 나현식, 최대선(숭실대학교)
	105	RansomFinder : 인공 지능을 이용한 랜섬웨어 탐지 홍석민, 김범현(한양대학교)
	112	스크린샷이 딥페이크 탐지 성능에 미치는 영향 박종우, 김지원(성균관대학교), 조철우, 윤성빈(대검찰청), 우사이먼성일(성균관대학교)
	114	사물인터넷 보안을 위한 배터리 상태 인지 파레토 전선 기반 동적 하이퍼파라미터 튜닝 기법 손규하, 김서이, 이일구(성신여자대학교)
10:30-11:30 (5-3) 인공지능 보안 X 좌장: 서승현 (한양대)	122	SDV 보안 강건성 향상을 위한 연합 학습 기반 NLU·LLM 프레임워크에 대한 연구 박준혁, 이재희, 안효범(국립공주대학교)
	245	Multi Agentic 프레임워크를 활용한 Data Source 기반 소스 코드 보안 진단 연구 남지우(중부대학교), 박영주(서울여자대학교), 이재훈(가천대학교), 이진규(전북대학교), 임형천(순천향대학교), 지한별, 최현우(성신여자대학교)
	249	Differential Evolution 기반 오류주입 파라미터 탐색 최적화 기법 제안 염지훈, 신원근, 박태윤, 김희석(고려대학교)
	309	A2A Multi-Agent System에서의 공격자 악성 작업 수행에 관한 사례 연구 전유경(중부대학교), 김지은(성신여자대학교), 이우진(소속없음), 임수환(순천향대학교), 조대인(전북대학교), 이유식(순천향대학교)
10:30-11:30 (5-4) SW/시스템 보안 III 좌장: 전승호 (가천대)	45	리눅스 커널 라이브러리(LKL)를 활용한 exFAT 파일 시스템 보안 취약점 탐지 고재훈(가천대학교), 권지훈(고려대학교), 한승훈(숭실대학교)
	63	HWTypeSan: ARM 포인터 인증 기반의 효율적인 타입 안전성 위반 취약점 탐지 도구 최민성, 전유석(고려대학교)
	183	Hardening Control-Flow Integrity via Program Context Concretization 변현수(서울과학기술대학교), 권용휘(메릴랜드대학교), 이창훈(서울과학기술대학교)
	217	안티탬퍼링 기술 보안성 평가 방법론 연구 이동호, 한지선, 조해현(숭실대학교)

구두발표 세션

2025년 11월 28일(금)		
세션	논문번호	논문제목(저자)
10:30-11:30 (5-5) IoT/CPS 보안 I 좌장: 박철준 (경희대)	44	Matter 프로토콜 취약점 분석 및 보안 연구 성준우(영남이공대학교), 한승훈(숭실대학교)
	59	드론 RF 무선 통신 시스템 설계를 위한 통신 장비 특성 분석 연구 지현태, 최상훈, 박기웅(세종대학교)
	165	IoT 펌웨어의 이종 경로 기반 분석 : Tapo C210 유예지, 김동인, 김대환, 박명서(한성대학교)
	206	Tangle 원장 기반 IoT 인증의 지연 안정화를 위한 앵커 크기 동적 제어 기법 윤현지, 유승우, 김수현(순천향대학교)
10:30-11:30 (5-6) 공급망 보안 I 좌장: 이만희 (한남대)	62	MITRE ATT&CK-D3FEND 지식 그래프 기반의 위협 대응 우선순위 모델 한희수, 최상훈, 박기웅(세종대학교)
	257	GitHub Actions의 신뢰 전이 모델링 및 정량적 위험 평가 방안 연구 조은정, 이만희(한남대학교)
	86	Comprehensive Analysis of Inaccurate OpenAPI Specifications in WordPress Plugins Grace Oluwabunmi Ohiremen, 김범현(한양대학교)
	251	AI 공급망 무결성 검증을 위한 블록체인 기반 Provenance 앵커링 프레임워크 연구 이준희, 이만희(한남대학교)
10:30-11:30 (5-7) 산업보안 좌장: 조효진 (연세대)	139	핵심 기반 시설 대상의 공격 시나리오 생성을 위한 MITRE CTI 통합 및 자동화 파이프라인 설계 노성현, 김태성(충북대학교)
	82	인터넷 연결 자산 및 위협 검색 기반선박 장비 원격 관리 인터페이스 취약점 분석 이진성, 나사랑, 김대운, 임준형(한국인터넷진흥원)
	106	사이버 복원력 측정을 위한 통합 평가 방안에 관한 연구 이새움, 최슬기, 김태현, 김서연, 오동환, 임준형, 김태은(한국인터넷진흥원)
	305	ADR 프레임워크: MITRE ATT&CK-D3FEND-CRR 연계 기반 사이버 회복력 진단 모델 이준용, 조리노, 강태영, 강정민(고려대학교)

구두발표 세션

2025년 11월 28일(금)

세션	논문번호	논문제목(저자)
11:40-12:40 (6-1) 정보보호 정책, 법, 제도 좌장: 홍준호 (성신여대)	149	국내외 표준 직무체계 분석을 통한 K-직무체계 (안)제안 : 정보보호를 중심으로 전효정, 박진용, 김태성(충북대학교)
	13	사이버 레인지 환경에서 훈련생의 인지 부하를 활용한 개인화 시나리오 추천 방법론 정상지, 박주선, 주한익, 홍순좌(코어시큐리티), 박성일(워크포스에이아이)
	55	사이버보안 훈련 시나리오 구조 및 표현 언어 제안 박현태, 이용균(내스타일)
	208	사이버레인지 기반 온라인 훈련 기반 정보보호 교육생 역량 측정 및 평가 실증 사례 강주영, 박혜민(한국정보보호산업협회)
11:40-12:40 (6-2) 이동통신 보안 좌장:서승현 (한양대)	247	국내 LTE/IMS 환경에서의 SMS 평문전송 및 도청 위험 실증 연구 이동원, 변민주(경희대학교), 최현영(엔에스원소프트), 박철준(경희대학교)
	202	IPsec 기반 5G Core-gNB 구간 인터페이스 보호 방안 연구 김영재, 원태호, 김보남, 유일선(국민대학교)
	266	5G 코어망 환경에서의 머신러닝 기반 트래픽 처리량 예측 최준서, 김민규, 김종현(세종대학교)
	220	이동통신환경에서 비식별 메타데이터 기반 IMSI Catcher 탐지 성능 비교 연구 서예린, 김준식, 김민규, 김종현(세종대학교)
11:40-12:40 (6-3) 모바일 보안 좌장: 김기윤 (대검찰청)	117	정적 분석 및 동적 분석을 통한 안드로이드 퍼징 하네스 생성 강민주, 이동하, 한규상, 박정우, 전승호(가천대학교)
	158	Android 환경에서 패스워드 매니저 Proton Pass의 암호화된 컨텐츠 복호화 및 아티팩트 분석 연구 강지현, 신지섭, 홍서현, 김종성(국민대학교)
	17	안드로이드 동적 분석 회피에 활용되는 커널 아티팩트 분석 고재휘, 김민재, 허준범(고려대학교)
	218	멀티 스레드 환경 안드로이드 어플리케이션 분석을 위한 Stacktrace 추적 기법 연구 윤성배, 박제만(경희대학교)
11:40-12:40 (6-4) SW/시스템 보안 IV 좌장: 윤주범 (세종대)	224	안티탬퍼링 시나리오 기반의 VFS 조사 및 식별 최재민, 허남정, 박준영(세종대학교), 장우현, 김연재, 허재원(LIG넥스원), 박기웅(세종대학교)
	225	MP FUSE: 리눅스 FUSE 기반 메타모픽/폴리모픽 변이 기술 최재민, 박준영, 허남정, 하영빈(세종대학교), 장우현, 김연재, 허재원(LIG넥스원), 박기웅(세종대학교)
	259	Analysis and bypass of F alco detection limits 표창우, 한승재, 주현석, 김창훈(대구대학교)
	128	정적 분석 기반 Rust 취약점 탐지 기술 동향 황승재, 조효진(연세대학교)

2025년 11월 28일(금)		
세션	논문번호	논문제목(저자)
11:40-12:40 (6-5) IoT/CPS 보안 II 좌장: 임재덕 (ETRI)	278	ICS에서의 ADT 기반 설명 가능한 이상징후 탐지 모델 구현 및 평가 이혜강, 이상원, 김수형, 하재철(호서대학교)
	301	Zigbee 기반 IoT 장치의 구현 취약점 탐지를 위한 능동적 OTA 퍼징 프레임워크 김민수, 조영효(서울과학기술대학교), 김역(전기정보기술연구소), 이창훈, 손기욱(서울과학기술대학교)
	285	GOTCHA! Drone: 드론의 무선 신호 취약점 분석을 위한 4단계 프레임워크 허남정, 최재민(세종대학교), 장우현, 김연재, 허재원(LIG넥스원), 박기웅(세종대학교)
	23	멀티센서 임베디드 시스템 검증을 위한 센서 데이터 시뮬레이션 기반 시험 프레임워크 최연준, 임재덕(한국전자통신연구원)
11:40-12:40 (6-6) 공급망 보안 II 좌장: 최대선 (숭실대)	260	ECSS-Q-ST Rev.2 보안 요구사항을 위한 실시간 운영체제 대상 SBOM 생성 김지민, 박주찬, 장준혁, 이만희(한남대학교)
	292	'Trusting Trust' 문제 완화를 위한 SBOM Generator 신뢰 검증 절차 연구 이준혁, 김지민, 이만희(한남대학교)
	204	소프트웨어 공급망 보안 강화를 위한 동적 바이너리 계측 기반 코드 클론 추적 방법 이경신, 이승광(단국대학교)
	261	빌드 환경 무결성 검증을 위한 CDXA 활용 방안 김지민, 이준혁, 이만희(한남대학교)
11:40-12:40 (6-7) 개인정보보호 좌장: 류권상 (국립공주대)	87	에이전틱 AI 기반 자율형 데이터 유출 방지 조항범, 오주엽, 박찬민, 최영락, 손현기, 윤명근(국민대학교)
	179	라즈베리 파이 기반 임베디드 환경에서의 BERT 계열 PII 마스킹 성능 비교 이범수, 고세화, 신다윗, 순준영(부산대학교)
	222	개인정보 보호 관점에서의 AI 브라우저 동작 메커니즘 분석: Comet의 Assistant 기능을 사례로 방재훈, 정수은, 박정흠(고려대학교)
	250	A Multi-Layer Hybrid Model for Detecting Personally Identifiable Information in Enterprise Documents Sobirova Khusnora Bakhtiyor Kizi, 이경현(부경대학교)

2025년 11월 27일(목)

세션	논문번호	제목(저자)
11:00~12:00 포스터 1 좌장: 주경호 (숭실대)	316	Minecraft에서 미끼 표적 비가시화를 통한 자동 공격 플레이어 탐지 방안 연구 가진섭, 지일환, 이주현, 서정택(가천대학교)
	8	Experimental Analysis of Same-Site Resource Exhaustion Attacks Based on the Browser Rendering Pipeline 변수민, 이웅희, 허준범(고려대학교)
	52	저궤도 군집 위성 네트워크의 양자내성암호 적용을 위한 보안 위협 및 기술적 요구사항 분석 권영은, 윤지원(고려대학교)
	85	메신저의 사용성 및 사용가능한 보안성 평가: 새로운 모델 제안을 기반으로 김태영, 오승준, 김승주(고려대학교)
	102	분산 제어 기반 군집 드론의 동적 환경 대응 성능 분석 노승덕, 박소희, 최대선(숭실대학교)
	136	사이버 위협 분석 자동화를 위한 ATT&CK 매핑 기법 비교 연구: BERT와 LLM 및 LLM-RAG 기반 접근 윤희서, 이윤서, 최은정(서울여자대학교)
	151	LTE 시스템의 취약점과 SMS 인증 의존성에 따른 국내 서비스 영향 분석 신유진, 박철준(경희대학교)
	156	AI-Driven Quantum Intrusion Detection and Resilience System (QIDS-R): From Error Correction to Security Aware 위비, 윤혜진, 이옥연(국민대학교)
	163	오류 주입 공격 취약 위치 평가를 위한 생성 파라미터 다양성 개선 방안 연구 김재효, 최기훈, 한동국(국민대학교)
	191	멀티 클라우드 보안 운영 효율화를 위한 통합 심각도 매핑 모델 연구 공나영, 김도영, 최상훈, 박기웅(세종대학교)
	244	해상 환경에서 디헤이징 객체 탐지 성능 향상을 위한 해무 데이터셋 생성 및 검증 연구 권순신, 권태경(연세대학교)
	302	uORB 메시지 기반 내부 이상 탐지 프레임워크 하영빈(세종대학교), 장우현, 김연재, 허재원(LIG넥스원), 박기웅(세종대학교)
	21	자기주권신원 보장을 위한 DID 기반 전자 투표 시스템 연구 오예선, 이기찬, 오수현(호서대학교)
	51	RAG 시스템에서의 데이터 포이즈닝 공격과 방어 연구 유승우, 김형식(성균관대학교)
	75	BSM 메시지 기반 리플레이 공격 경량 탐지 및 방어 프레임워크 김정현, 이세영(강원대학교)
	84	Agentic AI의 보안 위협과 대응 기술 분석 김다인, 김동현, 박성규, 최대선(숭실대학교)

포스터발표 세션

2025년 11월 27일(목)

세션	논문번호	제목(저자)
11:00~12:00 포스터 1 좌장: 주경호 (숭실대)	113	무음 파일 재생을 이용한 iOS 스마트폰 대상 은닉 채널 장진욱, 김용재, 한동국(국민대학교)
	138	sLLM(smaller Large Language Model) 기반 다중 소스 포렌식 증거 상관분석 프레임워크 나소진, 고세이, 김희정, 반영진, 이광호, 이민지, 이진웅, 김종민, 진필근(차세대 보안리더 양성 프로그램)
	142	A Model for Determining the Appropriate Privacy Level of De-identified Video/Image Data 최유정, 김태성(충북대학교), 어수행(크립토랩)
	184	클라우드 로그 기반 이상 행위 탐지 프레임워크 강대현, 김주영(한국외국어대학교), 김학범(홍익대학교), 박선하(아주대학교)
	201	딥러닝 모델 추출 공격의 연구 동향 (암호해독 기법 기반 가중치 복구를 중심으로) (형유림, 김덕연, 서효리, 이인화, 김은성, 석병진(한성대학교)
	236	딥페이크 탐지 최신 기술의 분류 및 동향 분석 이현석, 황은비, 권태경(연세대학교)
	267	Croissant 기반 데이터셋 메타데이터 정규화를 통한 결정론적 AI 모델 데이터 출처 검증 기법 김형규, 이만희(한남대학교)
	315	AI 에이전트를 활용한 N2SF 보안체계 적용 자동화 프레임워크 제안 김지원, 지일환, 이주현, 서정택(가천대학교)
	332	블록암호 AES의 CEJO 화이트박스 구현에 대한 BGE 기반 키 복구 공격 연구 김예진, 김동찬(국민대학교)
	9	PQC 서명 알고리즘 분석 및 전환 전략 김진섭, 송일환, 유지현(광운대학교)
	18	RFC 9794 분류 체계에 기반한 하이브리드 양자내성암호 기술 동향 서베이 우나륜, 유지현(광운대학교)
	27	대규모 멀티모달 생성형 모델에 대한 탈옥 공격 기술 동향 및 분석 김희환, 양홍장, 최대선(숭실대학교)
	40	변전소 운영자용 위협 모델: Modbus 기반 기만·물리조작 시나리오 최은지, 김혜민, 남보현, 류기현, 이상호, 전도현, 강대명, 김관영, 노용훈(KITRI BoB)
	54	Open-Vocabulary Video Anomaly Detection를 통한 미지정 이상 데이터 탐지 및 대응 설계 송다은, 김형식(성균관대학교)
	73	CNN 기반 게임 내 가격 정책별 소비 패턴 분석 이영상, 최지욱, 김윤호, 이명재, 김혜영(홍익대학교)
	119	LLM 기반 소프트웨어 취약점 분석 연구 동향 및 기술적 챌린지 분석 박정우, 강민주, 이동하, 한규상, 전승호(가천대학교)
	145	MCP 기반 AI 리버싱 환경의 새로운 공격 표면 분석 김현아, 홍득조(전북대학교)

2025년 11월 27일(목)

세션	논문번호	제목(저자)
11:00~12:00 포스터 1 좌장: 주경호 (숭실대)	187	글로벌 이커머스 플랫폼의 개인정보 국외이전 및 위탁 정책 자동 평가 시스템 서희연, 이준섭, 김태성(충북대학교)
	235	Leveraging the MITRE ATT&CK Framework for Developing an Automated SOC Ghaylan Fatih, Ghazi Fauzan, 최종욱(마크애니)
	258	BERT 기반 CAN 침입 탐지 시스템을 위한 교사 모델 개발 및 성능 검증 김경민, 박근희, 박준석, 전선우, 조후연(대구경북과학기술원)
	293	macOS 버전별 AUL 차이점 분석 김준영(백석대학교), 이정준(대구대학교), 강대명(Best of the Best)
	303	보안 경고 피로(Security Warning Fatigue)가 사용자 보안 행동에 미치는 영향: 연구 모형과 실증 계획 정재건, 김태성(충북대학교)
	317	LLM를 활용한 디컴파일러 연구 동향 조시은, 최원석(고려대학교)
	3	(EU) 2023/1230 규정 대비 산업 로봇 사이버 보안 프레임워크 제안: ISO 10218-1·IEC 62443-4-1, 4-2 매핑 기반 요구 사항도출 및 평가 배승연(한국에스지에스)
	89	인공지능 보안에서 블록체인의 역할에 대한 설문조사 아마다 유스릴 카딥티야, 레티투흐엉, 김희찬, 김호원(부산대학교)
	262	다중 에이전트 시스템의 공격 표면 분석을 통한 공격 벡터 도출 전지환(홍익대학교), 정민수(소속없음), 우승훈(울산대학교), 신현서(고려대학교), 이보겸(세종대학교), 박서영(고려대학교)
	291	딥페이크 이미지 생성기법별 최신 데이터셋 동향 분석 조원영, 황은비, 권태경(연세대학교)
	263	SAPIENS: Ontology, Graph RAG, Agentic AI를 통합한 지능형 Web3 보안 감사 시스템 설계 김진겸, 고남현, 이학성, 최민석, 이정현, 문병석(KITRI BoB)
	314	OCSF 기반 보안 로그 통합 분석 연구 문석환(인하대학교), 박혜수, 김미소(중부대학교), 박상경(인하대학교), 송지현, 어영민(중부대학교)
	281	GoJS를 활용한 개인정보 흐름도 자동 생성 모델 연구 손효림(서울여자대학교), 임창현(소속없음), 권다연(대전대학교), 박연서, 임지수(서울여자대학교)
	226	SCSC: 상호참조 기반 공급망 보안 관리체계 및 통합 플랫폼 제안 최하경, 유예서, 장인영, 이혜인(덕성여자대학교)

포스터발표 세션

2025년 11월 27일(목)

세션	논문번호	제목(저자)
13:00~14:00 포스터 2 좌장:김효승 (한림대)	319	미 국방부 제로 트러스트 보안 전략의 한국군 영향 분석 및 대응 방향 이지웅, 선희갑, 오경식(대한민국해군)
	47	WP-PROV: WordPress에서 W3C PROV 기반 출처 수집을 위한 파이프라인 이혁재, 박제만(경희대학교)
	68	A Survey and Comparative Analysis of Global AI Governance Based on the NIST AI Risk Management Framework 아크테르 모르셰다, 레티 투 흐엉, 이범수, 손준영(부산대학교)
	97	멀티클라우드 환경 간 IaC 이식성을 위한 AST 기반 생성형 AI 변환 기술 심예솔, 김서희, 김미진, 김성민(성신여자대학교)
	104	GNN 임베딩 기반 정상 유사 공격 데이터 선택을 이용한 백도어 공격 가능성 연구 안윤수, 장진혁, 남승수, 최대선(숭실대학교)
	92	Weaknesses of MMD-Regularized Backdoor Attacks and an Agent-Based Detection Method Leveraging Them 이진우, 신준석, 최대선(숭실대학교)
	152	다중 뉴럴 코덱 기반 화자인증 시스템의 적대적 공격 방어 효과 분석 서지원, 정수환(숭실대학교)
	157	제로트러스트 기반 OpenRAN 신원인증 아키텍쳐 제안 김대운, 박성민, 임준형(한국인터넷진흥원)
	181	Evolving Attack Tactics against Messaging Applications Shakhzod Yuldoshkhujaev, 이수연, 구형준(성균관대학교)
	231	ICS에서의 Isolation Forest 기반 이상징후 탐지 전원준, 안경덕, 기한결, 하재철(호서대학교)
	279	사이버 복원력 기반 취약점 우선순위 계량화 방법 강혜진, 조학수(호서대학교)
	15	프라이버시 강화를 위한 조건부 추적성을 제공하는 CBDC 모델 연구 이기찬, 오예선, 오수현(호서대학교)
	41	SIEM 환경의 이상 이벤트 우선순위 선별 연구 안소정(현대오토에버)
	65	입력 최적화를 위한 LLM 기반 ROS 퍼징 시스템 정우성, 김진하, 윤주범(세종대학교)
	79	안전한 옴니모달 AI 개발을 위한 보안 고려 사항 김동현, 박성규, 김다인, 최대선(숭실대학교)
	93	A Pareto Mini-Benchmark of Non-Learning-Based DWT+QIM Watermarking 이상윤, 이세영(강원대학교)

2025년 11월 27일(목)

세션	논문번호	제목(저자)
13:00~14:00 포스터 2 좌장:김효승 (한림대)	130	AI 기반 NIDS에 대한 모델 추출 공격 탐지 방법 김진성, 남승수, 최대선(숭실대학교)
	140	실수형 벡터 연산을 위한 영지식 증명 기법의 비교 연구 김재헌, 정익래(고려대학교)
	146	5G 네트워크 슬라이싱별 성능지표와 보안 요구사항의 상관관계 분석 정유진, 나승준, 김환국(국민대학교)
	190	LLM 기반 난독화 해독 및 네트워크 흐름 탐지와 UI 유사도 비교를 통한 피싱 사이트 탐지 시스템 설계 민준홍, 김서진, 원종현, 서준호, 남수만(청주대학교)
	207	국가 망 보안체계(N2SF) 내 AI 기반 등급분류 자동화 제안 이은진(세종대학교), 김민선(수원대학교), 이주오(명지대학교), 강석혁, 김수안(고려대학교), 박솔빈(홍익대학교), 곽승희(엔키화이트햇), 김수득, 이창선(김앤장 법률사무소)
	241	정보시스템 보안 모니터링을 위한 데이터 수집 및 정규화 기법에 관한 기초 연구: Windows와 Linux를 중심으로 전나현, 양희도, 윤우성, 박정흠(고려대학교)
	277	산업제어시스템 장비 펌웨어 기반 SBOM-VEX 연계를 통한 공급망 보안 강화 방안 연구 신용희, 고웅(한국인터넷진흥원), 엄익채(전남대학교)
	318	컨테이너 취약점에 따른 공격 벡터 식별 및 개선 연구 동향 김미연, 최상훈, 박기웅(세종대학교)
	6	Volumetric DDoS 방어 최신 동향과 Client Puzzle 기반 연구 방향 제시 이서영, 김범현(한양대학교)
	11	자동차 TARA 분석 과정의 객관화 및 일관성 확보 방법 박준호, 김찬민, 권민희(한국자동차연구원)
	20	거대 언어 모델 탈옥 공격 기법의 정량적 비교 연구 하지혁, 김혜빈, 한동식, 고민균, 최석환(연세대학교)
	35	Confiler: 컨테이너 환경을 위한 지능형 파일 접근 제어 프레임워크 박현준, 이승수(인천대학교)
	49	A study on Financial Circuit Breaker Mechanism for the Economic Stability of P2E Tokens Md Shariful Islam, 이원용, 박정민, 윤형균, 김혜영(홍익대학교)
	299	국가별 양자내성암호 전환 정책 비교 및 분석 노희원, 이상현, 장선우, 박가을, 서승현(한양대학교)
	78	5G 오픈소스 환경에서 DB 관리 실태와 개선 방안 추민호, 원태호, 김보남, 유일선(국민대학교)
	120	교란된 이미지 구별하기 위한 Siamese 신경망의 견고성 분석 안드로 아프릴라 아디푸트라, 레티투흐엉, 신다윗, 김호원(부산대학교)

포스터발표 세션

2025년 11월 27일(목)

세션	논문번호	제목(저자)
13:00~14:00 포스터 2 좌장:김효승 (한림대)	155	이진 필드 다항식 곱셈을 위한 butterfly 연산 병렬화 연구 김동천, 서석충(국민대학교)
	173	AI 편향성 완화를 위한 영지식 증명 기반의 투명성 거버넌스 제안 김민혜(한양대학교), 김지혜(국민대학교), 오현옥(한양대학교)
	198	하이브리드 AI 기반 다크패턴 탐지 및 분석 기법 연구 장세영(백석대학교), 정재웅(상명대학교), 이동훈(강원대학교), 최성훈(한국공학대학교), 전수경, 김유빈, 윤수연(이화여자대학교), 주영선(한국인터넷진흥원), 김경곤(나이프아랍안보과학대학교)
	243	ROS2 시스템의 퍼징 기법 연구 동향 이상진, 최원석(고려대학교)
	269	임베디드 시스템에 대한 퍼징 기법의 발전 동향 분석 임재형, 최원석(고려대학교)
	296	Purdue 모델 기반의 제로트러스트 아키텍처 적용 방향 분석 박소영, 목정현, 윤성우, 박지민, 이석준(가천대학교)
	304	탈중앙화 금융(DeFi) 환경에서의 실거래 데이터 기반 금융보안 리스크 분석 배준호, 박천호(고려대학교), 고철수(김앤장 법률사무소), 강형우(고려대학교)
	323	PCA 기반 행위-결과 융합형 랜섬웨어 탐지 방법 정일준, 정주현, 한승훈(숭실대학교)
	12	정적·동적 분석을 통한 양자취약암호(Non-PQC) 탐지도구 개발에 관한 연구 정진호(중부대학교), 서정민(중앙대학교), 신찬희(이화여자대학교), 하준수(한국항공대학교), 문재현(한국기술거래사회), 윤기순(NSHC)
	118	하이브리드 퍼징 연구 동향 및 기술적 챌린지 분석 한규상, 강민주, 이동하, 박정우, 전승호(가천대학교)
	274	ETSI TR 104 180 표준 기반 데이터 품질 평가 프레임워크 구현 표자연, 오예진, 이지은, 송재승(세종대학교)
	160	링크 선택과 프리엠블 타이밍 제어를 통한 통신 가용성 강화 김예신, 이진민, 이일구(성신여자대학교)
	282	멀티모달 센서 융합 시스템의 물리적 적대적 공격 취약성 분석 및 레질리언스 강화 방어 기술 동향 김가현, 최원석(고려대학교)
	29	해상 네트워크에서의 IDS 적용 가능성 연구: SCADA 환경과의 비교 분석 양승권, 정연서(중부대학교), 구지오(한경국립대학교)
	1	PoA 프라이빗 체인 브릿지의 보안성 및 TPS 향상 연구 김재현(건국대학교)
	288	블록체인 기반 개인정보보호 기술의 연구 동향과 통합적 발전 방향 오예진, 표예진, 이지은, 송재승(세종대학교)

2025년 11월 27일(목)

세션	논문번호	제목(저자)
14:10~15:10 포스터 3 좌장: 이윤호 (서울과기대)	331	퍼미션드 블록체인에서 PQC 서명 검증 동향 김현준, 서화정(한성대학교)
	48	임베디드 웹 서버를 위한 경량화된 적응형 하이브리드 보안 아키텍처 설계 곽수민, 박병우, 남보현(국립한밭대학교)
	71	HIERA Detector: NIDS 적대적 백도어 탐지를 위한 트랜스포머 표현값의 계층적 클러스터링 장진혁, 안윤수, 김진성, 최대선(숭실대학교)
	98	피싱 url의 단기 생존 특성 분석 및 조기 예측 모델 곽나영(명지대학교), 서민재(국립한밭대학교), 정윤성(세종대학교), 이동우(한국기술교육대학교), 박수성(전남대학교), 류현(청주대학교), 이경문(이스타미디어), 전상현(악성코드검거단)
	109	피지컬 네트워크 환경에서 전송 트래픽을 활용한 NIDS 모델추출공격 오윤주, 김도완, 민동욱, 최대선(숭실대학교)
	147	CTI 기반 탐지 정책 자동 생성 연구 동향 유진호, 조효진(연세대학교)
	153	ATB-Insider: 시계열 이상 탐지를 활용한 실시간 내부자 위협 탐지 모델 김가영, 박나은, 이일구(성신여자대학교)
	162	Montgomery Multiplication을 통한 Microsoft SEAL-Embedded 라이브러리 최적화 김채린, 김영범, 서석충(국민대학교)
	185	인공지능 생성 텍스트 워터마킹 기법 분석 권기욱, 김민석, 구형준(성균관대학교)
	242	전기차 BMS에 대한 EMI 신호 주입 공격 연구 동향 (Trends in Electromagnetic Interference-Based Signal Injection Attacks Targeting Battery Management Systems in Electric Vehicle) 김진세, 최원석(고려대학교)
	297	Exploring Potential Security Threats to Virtual Power Plants 서유정, 한슬기, 이현우(KENTECH)
	14	양자내성암호 전환을 위한 멀티-에이전트 LLM 프레임워크에 관한 연구 하준수(한국항공대학교), 정진호(중부대학교), 서정민(중앙대학교), 신찬희(이화여자대학교), 문재현(한국기술거래사회), 윤기순(NSHC)
	46	스캐닝 이벤트의 재해석과 가치 복권: 엔터프라이즈 방어를 위한 체계적 모델 제안 이효진(현대오토버)
	69	자율주행 시스템의 분포 외 탐지: 방법 및 벤치마크 레티투흐엉, 장현진, 김호원(부산대학교)
	80	오디오 워터마킹에서의 시간 스트레칭 공격 대응을 위한 시간 반전 기법 박성호, 정수환(숭실대학교)
	96	다중 모듈 융합 멀티 스캐너를 이용한 알려지지 않은 악성 URL 탐지 서민재(국립한밭대학교), 이동우(한국기술교육대학교), 박수성(전남대학교), 류현(청주대학교), 정윤성(세종대학교), 곽나영(명지대학교), 이경문(이스타미디어), 전상현(악성코드검거단)

2025년 11월 27일(목)

세션	논문번호	제목(저자)
14:10~15:10 포스터 3 좌장: 이윤호 (서울과기대)	132	전송보안을 위한 주파수 도약 알고리즘 설계 이창민, 권희진, 추요한, 안재만, 오석근, 유지원(고려대학교), 설영욱(쎄트렉아이), 최두호(고려대학교)
	141	랜섬웨어 암호화 구조 및 공격 전략의 시기별 진화 분석 유현준, 유지현(광운대학교)
	172	인증 취약점 기반 EV 충전소 공격 시나리오 김태우, 레리사 아데바 질차, 송유래, 김득훈, 곽진(아주대학교)
	193	CKKS 기반 동형 ML 구현을 위한 활성화 함수 근사 방법론 조사 연구 신호준, 이윤호(서울과학기술대학교)
	209	PPRL 벤치마킹을 위한 NCVR 데이터셋의 체계적 활용 연구 이민호, 전영준, 김효승(한림대학교)
	256	위협모델링을 통한 MCP AI Agent 보안 요구사항 도출 김은서(고려대학교), 도현정, 안현수, 이민혁, 이정헌, 장다연(한국정보기술연구원 차세대 보안리더 양성 프로그램), 권헌영(고려대학교)
	283	국산 블록암호의 양자 구현과 분석 동향 신다윗, 조재한, 김호원(부산대학교)
	330	MITRE ATT&CK 기반 주요 클라우드 벤더별 공격 표면 및 공격 벡터 비교 분석 지동혁, 최상훈, 박기웅(세종대학교)
	7	RSSI 보조를 통한 BLE 기기의 안정적 RFFI 기반 식별 및 주적 기법 이경한, 최경록, 허준범(고려대학교)
	176	합성물의 개인정보보호법상 정의 및 법적 함의 제안 김여진, 김아람(수원대학교)
	25	보안 기술개발 지원을 위한 실-가상 연동 V2X 시험환경 개발 박채훈, 김찬민, 권민희(한국자동차연구원)
	38	OpenRAN 아키텍처 Near-RT RIC 보안 연구 동향 분석 이준희, 주경호(숭실대학교)
	53	대규모 언어모델 백도어 공격 및 방어 기법 비교 분석 박준형, 김형식(성균관대학교)
	61	인공지능을 활용한 다크패턴 탐지 시스템 박선하, 신은별, 유채연, 이윤희(아주대학교)
	116	Security Technology Trends for AI Agents 김현지, 윤세영, 서화정(한성대학교)
	64	Inputless Receiver가 결과를 획득하는 MPSU에 관한 연구 김기환, 김수현, 이임영(순천향대학교)

2025년 11월 27일(목)

세션	논문번호	제목(저자)
14:10~15:10 포스터 3 좌장: 이윤호 (서울과기대)	169	도심빌딩 내 위험 상황 자동 인식 및 대응을 위한 보안 서비스 시나리오 개발 백영현, 김석윤, 임준규, 김창후, 이준명(유니온바이오메트릭스)
	174	Operational Performance Analysis of Deep Learning-Based Intrusion Detection for Cloud-Native 5G Core Networks 주리 라스트레, 빈센트 아벨라, 줄리아완 아디, 이동훈, 김보남, 유일선(국민대학교)
	10	제로트러스트 베이스라인 도입 방안과 진단 및 개선 체계 제안 백승렬(국민대학교), 오세희(서울여자대학교), 홍혜원(수원대학교), 김채은, 안현선(중앙대학교), 현석훈(LG CNS), 김두민(SK텔레콤), 문광석(코리안리재보험)
	252	중간 표현 및 LLM을 이용한 바이너리 정적 분석 및 취약점 패치 자동 탐지 시스템 지연태, 김찬인, 최승혁, 차우찬, 이유식(순천향대학교)
	270	OpenChain AI-SBOM 컴플라이언스 관리 가이드라인 분석 이은섭, 이만희(한남대학교)
	300	클라우드 공유 링크에 대한 잠금 해제 방안 김성우, 최대호, 조민정, 김역, 손기욱, 이창훈(서울과학기술대학교)
	312	O-RAN 환경에서 악성 xApp에 의한 보안 취약점 동향 및 추가 고려사항 박지민, 목정현, 윤성우, 박소영, 이석준(가천대학교)
	327	HStreamer:고대역폭 비동기 암호화 스트리밍 서버 김태희, 서건호, 조학수(호서대학교)
	94	BT-SSC: 블루투스 환경을 위한 X.509 인증서 구조 배우리, 강규현, 윤택영(단국대학교)
	200	Quantum money 연구 동향 송경주, 서화정(한성대학교)
	276	개인정보 영향평가 민간 확대 방안 및 수행안내서 제안 손효림(서울여자대학교), 임창현(소속없음), 권다연(대전대학교), 박연서, 임지수(서울여자대학교)
	170	Side-Channel Attack과 대응 기법에 대한 조사 정성윤, 서지원(단국대학교)
	295	macOS AUL 기반 행위 탐지 모니터링 시스템 김현진(아주대학교), 박준언(조선대학교), 유은서(숙명여자대학교), 강대명(Best of the Best)
	271	비정형 텍스트 데이터의 개인정보 탐지를 위한 패턴-LLM 하이브리드 방법론 김수정, 장대일(한국인터넷진흥원)
	2	정형기법 기반 보안 프로토콜 자동화 검증 도구 사용자 인터페이스 제공 방법 최민석, 하수정, 임재덕(한국전자통신연구원)

학술대회 등록방법

◈ 등록비

구분	회원	비회원	현장등록
일반	300,000원	400,000원	400,000원
군 / 공무원	200,000원	250,000원	250,000원
학생(전일제)	150,000원	200,000원	200,000원
시니어(63세이상) 종신회원	무료		

* 등록비 포함 사항: 행사 기간 중 제공되는 식사, 리플릿, 온라인 프로시딩, 기념품

〈제공 식사〉

11월 27일(목) 중식 및 석식(만찬)

11월 28일(금) 조식 및 중식

- 군/공무원 등록은 주무관청에 소속 중인 공무원증 소지자에 한합니다. (국공립 교직원 제외)
- 시니어 무료등록은 학회 종신회원으로 1963년 12월 31일 이전 출생자에 한합니다.
- 학회 특별회원사 임직원은 학회 회원으로 준합니다. 특별회원사 여부는 학회 홈페이지 (www.kiisc.or.kr) 회원광장 → 특별회원사에서 확인하실 수 있습니다.
- 회원가 혜택 기준은 행사 당일인 2025/11/27(목)까지 '활동 회원(연회비 납부 회원)'이어야 합니다.
- 학생은 학부생/대학원생 전일제에 한합니다. (타소속 없음)
- 논문 한편당 저자 한 분은 반드시 사전 등록을 하셔야 합니다.

[사전등록]

- 학회 홈페이지(www.kiisc.or.kr)에서 접속할 경우, 학회행사 → 사전등록바로가기 → 학술행사 선택(2025 동계학술대회) 등록하기 선택
- 사전등록 마감일
  - 발표자 사전등록: ~2025년 11월 13일(목)까지
  - 참가자 사전등록: ~2025년 11월 17일(월)까지
- 계좌번호: 국민은행 754-01-0008-146 (예금주 한국정보보호학회)
- 무통장 입금 결제 시 등록비는 위 계좌로 송금하시고, 입금자가 대리일 경우 통보 바랍니다.
- 신용카드 결제 시 계산서 발급이 불가합니다. (부가가치세법 시행령 제57조)
- 사전등록 시 (2-3일 이내) 기재해주신 이메일로 청구용 계산서가 발행되오니 영수용 계산서가 필요하신 경우 미리 학회로 연락바랍니다.
- 참가확인서는 등록비를 완납하신 분에 한하여 발급 가능합니다.
  한국정보보호학회 홈페이지 상단의 「행사등록 및 참가확인서」 바로가기를 클릭하신 후, 등록 시 입력한 성함과 이메일 주소를 동일하게 입력하시면 출력하실 수 있습니다. (단, 참가확인서는 행사종료 후 다음날부터 발급 가능)

[계산서 문의처]

- 한국정보보호학회 사무국 02-564-9333(내선5), kiisc@kiisc.or.kr

[행사 문의처]

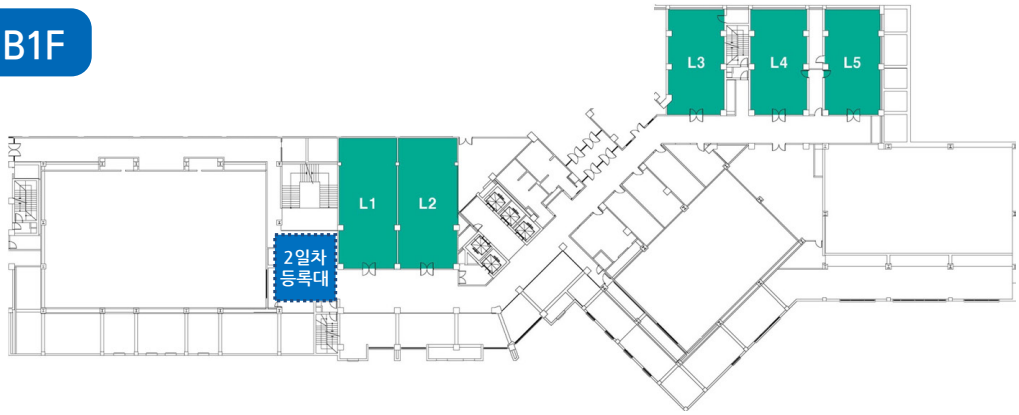
- 한국정보보호학회 사무국(등록 및 행사 진행) 02-564-9333(내선3), kiisc@kiisc.or.kr
- 한국정보보호학회 사무국(논문) 02-564-9333(내선1), kiisc@kiisc.or.kr

행사장소 안내

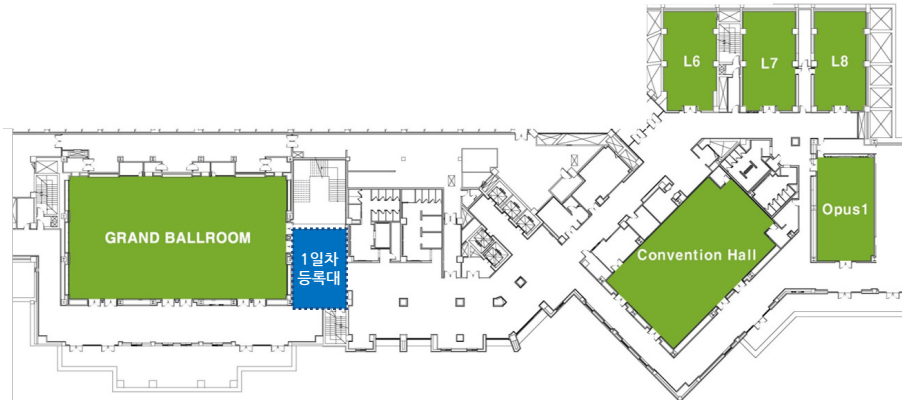
◈ 주요 행사 및 프로그램 장소 안내

E/W빌리지 1F

E/W빌리지 B1F



E/W빌리지 B2F



	E/W빌리지 (B2F)				E/W빌리지 (B1F)	E/W빌리지 (1F)	
	Grand Ballroom	Convention Hall	L6~L8	OPUS1	L1~L5	M7~M8	M6
DAY1 (11/27, 목)	개회식/ 정기총회/ 만찬(학생)	포스터 세션	논문발표	운영대기실	논문발표		
DAY2 (11/28, 금)					논문발표	논문발표	운영대기실

※ 등록대 위치 변경 안내
1일차(11/27, 목): 지하 2층 그랜드 볼룸 앞 | 2일차(11/28, 금): 지하 1층 계단 옆, 컨퍼런스 L1 옆

※ 개회식 종료 후 경품 추첨이 진행될 예정입니다.
경품추첨 (갤럭시 탭 S11(1개), 갤럭시 버즈 프로3(3개), 스타벅스 상품권(10매))

행사장소 안내

◈ 식사 제공 및 장소 안내

일자	내용	시간	장소
11/27 (목)	중식	12:00~13:00	카페테리아 (스키하우스 2F)
	만찬	19:00~	[일반] 미라시아 (빌리지센터 1F), [학생] 그랜드 볼룸 (E/W빌리지 B2F)
11/28 (금)	조식	08:00~09:00	카페테리아 (스키하우스 2F)
	중식	12:40-14:00	[일반] 미라시아 (빌리지센터 1F), [학생] 카페테리아 (스키하우스 2F)

※ 명찰에 포함된 식사권을 제출하신 후 식사 이용이 가능합니다. 식사권은 재발급이 불가하오니 반드시 지참해주시기 바랍니다.

◈ 단체행사 지상 차량등록

• 학술대회 홈페이지 행사장 안내 하단에 링크에 들어가시어 주차 등록을 하시면 지상 주차 무료입니다.
www.cisc.or.kr → 숙박/주차 내 URL 참고

※ 곤지암리조트 내 주차를 원하시는 일반 참가자(숙박X)께서는 입차 전 차량등록을 반드시 완료해 주시기 바랍니다.
차량등록이 완료된 경우에만 지상주차장 차단바가 자동으로 열려 주차가 가능합니다.
(차량 미등록 시 진입 불가, E/W빌리지 지하는 주차 불가(투숙객 전용))

※ 숙박(투숙객)자분들께서는 리조트에서 별도로 발송 드린 문자 내 URL에 접속하시어 사전에 차량을 등록하셔야만 지하, 지상 모두 무료 주차가 가능합니다.

- 예약번호: 24945505
- 고 객 명: 한국정보보호학회
- 행 사 명: 한국정보보호학회
- 행사일자: 2025-11-27~2025-11-28
- 차량등록 야외 주차장 위치 : 5, 6, 7번 주차장(차량 미 등록 시 이용불가)

MEMO


2025년 한국정보보호학회 동계학술대회
CISC-W'25
Conference on Information Security and Cryptography Winter 2025
2025년 11월 27일(목)~28일(금) | 곤지암리조트