한국정보보호학회
Korea Institute of Information Security & Cryptology

2024년 한국정보보호학회 동계학술대회

CISC-W'24

Conference on Information Security and Cryptography Winter 2024

2024년 11월 28일(목)~29일(금)

곤지암 리조트

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, LIG

위원회

학술대회장

한국정보보호학회 회장 하재철 (호서대학교)

조직위원회

- 조직위원장: 원유재 (충남대학교)
- 조직위원: 김원호 (국가보안기술연구소), 김정녀 (한국전자통신연구원), 김호원 (부산대학교), 박영호 (세종사이버대학교), 송중석 (한국과학기술정보연구원), 오진영 (한국인터넷진흥원)

프로그램 위원회

- 프로그램위원장: 권태경 (연세대학교)
- 프로그램위원: 강민석 (KAIST), 곽 진 (아주대학교), 곽병일 (한림대학교), 구형준 (성균관대학교), 권동현 (부산대학교), 김동우 (동국대학교), 김득훈 (아주대학교), 김범현 (한양대학교), 김성욱 (서울여자대학교), 김수현 (순천향대학교), 김종길 (이화여자대학교), 김종성 (국민대학교), 김형식 (성균관대학교), 김형종 (서울여자대학교), 김호원 (부산대학교), 김환국 (국민대학교), 김휘강 (고려대학교), 김희석 (고려대학교), 류권상 (공주대학교), 박기웅 (세종대학교), 박승현 (한성대학교), 박종환 (상명대학교), 박철준 (경희대학교), 배 호 (이화여자대학교), 변진욱 (평택대학교), 서석충 (국민대학교), 서정택 (가천대학교), 서지원 (단국대학교), 서화정 (한성대학교), 양대헌 (이화여자대학교), 우사이먼 (성균관대학교), 유일선 (국민대학교), 유지현 (광운대학교), 윤명근 (국민대학교), 윤종희 (영남대학교), 윤택영 (단국대학교), 이광수 (세종대학교), 이덕규 (서원대학교), 이만희 (한남대학교), 이문규 (인하대학교), 이병영 (서울대학교), 이선우 (서울여자대학교), 이세영 (강원대학교), 이연준 (한양대학교), 이일구 (성신여자대학교), 이종혁 (세종대학교), 이창훈 (서울과학기술대학교), 이태진 (호서대학교), 이현우 (한국에너지공과대학교), 임을규 (한양대학교), 장대희 (경희대학교), 장진수 (충남대학교), 장항배 (중앙대학교), 전상훈 (국민대학교), 정익래 (고려대학교), 조남수 (단국대학교), 조효진 (연세대학교), 주경호 (숭실대학교), 최대선 (숭실대학교), 최선오 (전북대학교), 최원석 (고려대학교), 최윤호 (부산대학교), 허준범 (고려대학교), 홍득조 (전북대학교), 홍석희 (고려대학교), 황성재 (성균관대학교)

운영위원회

- 운영위원장: 한동국 (국민대학교)
- 운영위원: 강유성 (한국전자통신연구원), 김소정 (국가안보전략연구원), 김은영 (국가보안기술연구소), 고광만 (SSNC), 박명서 (한성대학교), 김태규 (LIG넥스원), 박정수 (강남대학교), 박애선 (방첩사령부), 이도훈 (국가보안기술연구소), 방혁준 (쿤텍), 이상만 (고려대학교), 이봉수 (국가보안기술연구소), 장상운 (국가보안기술연구소), 임재덕 (한국전자통신연구원), 정치곤 (방첩사령부), 조해현 (숭실대학교), 최두호 (고려대학교), 지재덕 (국민대학교), 한찬희 (H2C글로벌), 한미란 (고려대학교))

(최)우수논문

번호	상장	논문번호	논문명	저자
1	과학기술정보통신부 최우수논문상	209	CCS 기반 전기차 충전 시스템에 대한 은밀한 서비스 거부(DoS) 공격	박유희, 김주언, 최원석(고려대학교)
2	행정안전부 최우수논문상	170	고사양 장비에 대한 상관 전자파 분석	김주환, 한동국(국민대학교)
3	학회 최우수논문상	149	kpqm4: KpqC 공모전 알고리즘에 대한 ARM Cortex-M4 벤치마킹 프레임워크	최용렬, 서석충(국민대학교)
4	학회 최우수논문상	270	모아레 패턴이 딥페이크 탐지 성능에 미치는 영향	허민지, Razaib Tariq, 우사이먼 성일(성균관대학교)
5	한국인터넷진흥원 우수논문상1	205	ARADI 암호의 바이트 동일 특성	김선엽, 김선규,신명수, 김인성, 신한범, 권동근, 석병진(고려대학교), 이동재(강원대학교), 홍득조(전북대학교), 성재철(시립대학교), 홍석희(고려대학교)
6	한국인터넷진흥원 우수논문상2	105	영어 및 한국어 탈옥 완화 템플릿을 활용한 PromptGuard의 탐지 성능 및 실효성 분석	나현식, 박성호, 윤두식, 최대선(숭실대학교)
7	한국전자통신연구원 우수논문상1	146	차량 네트워크의 비정상 행위 탐지를 위한 LSTM-PacGAN 모델	이민종, 김수형, 하재철(호서대학교)
8	한국전자통신연구원 우수논문상2	122	CLIP 모델 미세 조정을 통한 제로샷 기반 딥페이크 탐지 성능 향상 연구	이재희, 권태경(연세대학교)
9	국가보안기술연구소 우수논문상1	102	ICS 데이터를 활용하는 설명가능한 멀티모달 기반 단계적 사이버 공격 탐지 모델 제안	이주현, 전승호, 서정택(가천대학교)
10	국가보안기술연구소 우수논문상2	235	T-depth 및 KQ_T 측면 효율적인 양자 제곱 회로 설계	조성민, 이창열, 서승현(한양대학교)
11	한국과학기술 정보연구원1	135	자율 주행 차량의 차선 인식 알고리즘에 대한 적외선 활용 공격 기술 제안	주현민, 우상민, 김도현, 최원지, 김재훈, 김용대(KAIST)
12	한국과학기술 정보연구원2	204	Log Dataset Distributional Variability and its Implication for Robust Log Anomaly Detection	Lelisa Adeba Jilcha, 김득훈, 곽진(아주대학교)
13	학회 우수논문상	197	쇼어 알고리즘 최적화를 위한 양자 회로에서의 연산 알고리즘 구현	조재한, 신다윗, 김호원(부산대학교)
14	학회 우수논문상	30	메모리 분석을 통한 데이터베이스 정보유출 위험성에 대한 연구	오상원(에이치엠컴퍼니), 서종찬(청주대학교), 손석훈(서원대학교), 우현우(대구가톨릭대학교), 이덕규(서원대학교)
15	학회 우수논문상	139	IoT 환경을 위한 암시적 인증서 기반 KEM-TLS	한윤선, 서석충(국민대학교)
16	학회 우수논문상	104	AES 기반 AEAD 스킴의 키 커밋 공격 복잡도 계산	김선규, 신명수, 신한범, 김인성, 김선엽, 권동근, 석병진(고려대학교), 이동재(강원대학교), 홍득조(전북대학교), 성재철(서울시립대학교), 홍석희(고려대학교)
17	학회 우수논문상	268	증명 가능한 안전성을 지닌 고속 AES S-Box 고차 마스킹	안현준, 한동국(국민대학교)
18	학회 우수논문상	72	AVX2와 VPCLMULQDQ 명령어를 활용한 HQC의 GF(2)[x] 다항식 곱셈 최적화	장지훈, 이명훈(고려대학교), 김수리(성신여자대학교), 홍석희(고려대학교)
19	학회 우수논문상	151	대규모 언어모델 한국어 탈옥 프롬프트 분류기 연구	박대얼, 장현준(숭실대학교), 윤두식(이로운앤컴퍼니), 최대선(숭실대학교)

번호	상장	논문번호	논문명	저자
20	학회 우수논문상	62	효율적인 멀웨어 분석을 위한 Markov-CNN 기반 바이너리 난독화 기법 분류	강준혁, 이지원, 진홍주, 최원석, 이동훈(고려대학교)
21	학회 우수논문상	103	임베디드 기기의 암호화된 펌웨어 이미지 복호화 기법 연구	이철한, 정수은, 박정흠(고려대학교)
22	학회 우수논문상	145	DNN 모델 보호를 위한 전적 분할되고 효율적인 인스트럭션 추적 기반 모니터링 하드웨어	송용호, 우병수, 한영광, 강병훈(KAIST)
23	학회 우수논문상	41	USB 드라이버 퍼징을 위한 장치 프로토콜 규격의 자동 생성	강민석, 송도경(연세대학교)
24	학회 우수논문상	186	차세대 지능형 교통시스템 이상탐지 실증 연구	김지수, 장승현, 최유나, 김현민, 신재혁, 윤명근(국민대학교)
25	학회 우수논문상	192	리눅스 기반 런타임 타입 SBOM 생성 방법과 구현	손현승, 김지민, 이만희(한남대학교)
26	학회 우수논문상 (학부생)	257	불법 콘텐츠 배포 방지를 위한 CNN 기반 딥 페이크 탐지 기술	조경수, 문지윤, 오준희, 이종혁(세종대학교)
27	학회 우수논문상 (학부생)	196	차분 및 선형 공격에 대응을 위한 경량 암호 MGFN의 필요 라운드 수 분석	김남일, 송원우, 전용진, 백승준, 김종성(국민대학교)
28	학회 우수논문상 (학부생)	250	KpqC 2라운드 후보 TiMER의 메시지 인코딩에 대한 단일파형공격	유성환, 한재승, 한동국(국민대학교)
29	학회 우수논문상 (학부생)	245	차세대 Military-BcN과 5G 상용망 연동 시 모바일 업무 환경 보안 기법 연구	김찬혁, 김형엽, 위한샘, 이옥연(국민대학교)
30	학회 우수논문상 (학부생)	31	최신 ASV 적대적 공격의 문제점 고찰 및 개선방안 제안	이요원, 홍기훈, 정수환(숭실대학교)

11월 28일 (목)

시간	구두트랙1 컨퍼런스 L1 (B1F)	구두트랙2 컨퍼런스 L2 (B1F)	구두트랙3 컨퍼런스 L3 (B1F)	구두트랙4 컨퍼런스 L4 (B1F)	구두트랙5 컨퍼런스 L5 (B1F)	구두트랙6 OPUS 2 (B1F)	포스터세션 그랜드볼룸 앞 (E빌리지 B2F)
10:00~11:00	참가자 등록 그랜드볼룸 앞 (E빌리지 B2F)						
11:00~12:00	좌장: 이유석 (ETRI)	좌장: 구형준 (성균관대)	좌장: 조효진 (연세대)	좌장: 이현우 (KENTECH)	좌장: 이재승 (NSR)	좌장: 이일구 (성신여대)	좌장: 김효승 (한림대)
	(1-1) 양자보안 I	(1-2) 인공지능과 보안 I	(1-3) 모빌리티 보안 I	(1-4) 해킹과 취약점 분석 1	(1-5) IoT/로봇보안	(1-6) 제로 트러스트/ 네트워크 보안	Poster Session I
12:00~13:00	중식 카페테리아 (스키하우스 2F)						
13:00~14:00	좌장: 노동영 (NSR)	좌장: 심규석 (KISTI)	좌장: 이원혁 (KISTI)	좌장: 박기웅 (세종대)	좌장: 구본욱 (NSR)	좌장: 유지현 (광운대)	좌장: 곽병일 (한림대)
	(2-1) KpqC	(2-2) 인공지능과 보안 II	(2-3) 모빌리티 보안 II	(2-4) 해킹과 취약점 분석 II	(2-5) 암호이론과 구현 I	(2-6) 금융보안/정보보호 정책, 법, 제도	Poster Session II
14:00~14:10	휴식						
14:10~15:10	좌장: 임재덕 (ETRI)	좌장: 진승헌 (ETRI)	좌장: 한상윤 (NSR)	좌장: 서화정 (한성대)	좌장: 장상운 (NSR)	좌장: 이태진 (호서대)	좌장: 한미란 (고려대)
	(3-1) 양자보안 II	(3-2) 인공지능과 보안 III	(3-3) 모바일 보안/ 소프트웨어 보안	(3-4) 네트워크보안	(3-5) 디지털 포렌식/ 취약점 분석 1	(3-6) 기업소개 및 채용상담 LIG넥스원, 현대모비스	Poster Session III
15:10~15:40 (30분)	신진연구자 소개 세션 (좌장: 한양대 서승현) 그랜드볼룸 (E빌리지 B2F) 신진연구자: 한국에너지공과대 이현우, 서울여대 이선우, 단국대 서지원, 경희대 박철준						
15:40~16:10 (30분)	초청강연 (좌장: 연세대 권태경) AI의 국내외 입법 동향과 시사점/장준영 (AI센터장/변호사 법무법인 세종) 그랜드볼룸 (E빌리지 B2F)						
16:10~16:20	휴식						
16:20~17:00 (40분)	개회식 그랜드볼룸 (E빌리지 B2F)						
	사회: 김소정 (INSS) 국민의례 내빈소개 개회사 : 한국정보보호학회 하재철 회장 환영사 프로그램위원장 행사보고 (최)우수논문 시상 경품 추첨 (스타벅스 상품권)						
17:00~17:10	휴식						
17:10~18:30	정기총회 그랜드볼룸 (E빌리지 B2F)						
19:00~	만찬 학생 : 그랜드볼룸 앞 (E빌리지 B2F), 일반 : 미라시아 (빌리지센터 1F)						

11월 29일 (금)

시간	구두트랙1 컨퍼런스 L1 (B1F)	구두트랙2 컨퍼런스 L2 (B1F)	구두트랙3 컨퍼런스 L3 (B1F)	구두트랙4 컨퍼런스 L4 (B1F)	구두트랙5 컨퍼런스 L5 (B1F)
08:00~09:00	조식 카페테리아 (스키하우스 2F)				
09:00~09:30	참가자 등록 그랜드볼룸 앞 (E빌리지 B2F)				
09:30~10:30	좌장: 석우진 (KISTI)	좌장: 김수현 (순천향대)	좌장: 이만희 (한남대)	좌장: 박정수 (강남대)	좌장: 김득훈 (아주대)
	(4-1) 양자보안 III	(4-2) 인공지능과 보안 IV	(4-3) 블록체인 보안	(4-4) 산업보안/모바일보안	(4-5) 웹 서비스 보안
10:30~10:40	휴식				
10:40~11:40	좌장: 서석충 (국민대)	좌장: 심보연 (ETRI)	좌장: 박소희 (ETRI)	좌장: 박명서 (한성대)	좌장: 이새움 (KISA)
	(5-1) 하드웨어 보안	(5-2) 부채널 보안 I	(5-3) 인공지능 / 기타 정보보안	(5-4) 공급망 보안	(5-5) 공공 인프라 보안
11:40~13:00	중식 카페테리아 (스키하우스 2F)				
13:00~14:00	좌장: 김소정 (INSS)	좌장: 김은영 (LIGNEX1)	좌장: 박철준 (경희대)	좌장: 전상훈 (국민대)	좌장: 김종성 (국민대)
	(6-1) 개인정보보호	(6-2) 부채널 보안 II	(6-3) 시스템 보안	(6-4) 학부생 우수 논문	(6-5) 디지털 포렌식/ 취약점 분석 II

2024년 11월 28일 (목)

세션	논문번호	논문제목(저자)
11:00~12:00 (1-1) 양자보안 I 좌장: 이유석 (ETRI)	235	T-depth 및 KQ_T 측면 효율적인 양자 제곱 회로 설계 조성민, 이창열, 서승현(한양대학교)
	200	NTRU계열 암호 기법의 복호화 실패율 제어 방법 비교 분석 곽현지, 김종현(고려대학교), 박종환(상명대학교)
	50	Quantum Error Resilience Enhancement with Shor Code 위비, 윤혜진, 이옥연(국민대학교)
	65	가역 논리 합성을 통한 양자 회로 합성 및 구현 최찬호, 오진섭, 이상만, 최두호(고려대학교)
	46	양자내성암호 기반 TLS 1.3 동향 분석 김현주, 정수용, 홍도원, 서창호(공주대학교)
11:00~12:00 (1-2) 인공지능과 보안 1 좌장: 구형준 (성균관대)	234	컨볼루션 신경망에 대한 자가 오류 주입 탐지 신경망 김주환, 한동국(국민대학교)
	191	합성데이터 생성 연구 동향 전민선, 우사이먼성일(성균관대학교)
	171	분류 인공지능 기반 오류 주입 공격 파라미터 생성 방안 김주환, 한동국(국민대학교)
	57	VEXine: Automating SBOM and VEX Generation Using Transformer LLM Models 윤수연, 김윤지(이화여자대학교), 권민주(순천향대학교), 박종원(동국대학교), 김상범(김포대학교)
	62	효율적인 멀웨어 분석을 위한 Markov-CNN 기반 바이너리 난독화 기법 분류 강준혁, 이지원, 진홍주, 최원석 , 이동훈(고려대학교)
11:00~12:00 (1-3) 모빌리티 보안 I 좌장: 조효진 (연세대)	226	차량 환경에서의 감사데이터 검증 기법 박수연, 전희도, 최원석(고려대학교)
	186	차세대 지능형 교통시스템 이상탐지 실증 연구 김지수, 장승현, 최유나, 김현민, 신재혁, 윤명근(국민대학교)
	71	차량용 이더넷에 적용 가능한 보안 프로토콜 분석 이경연, 최원석(고려대학교)
	114	CNN-LSTM 기반 자동 운반 차량의 운행 데드락 탐지 시스템 이승열, 이상원(호서대), 정영래, 김희찬(OpenSG), 하재철(호서대)
	116	주행 환경 돌발 검출 알고리즘 구현 정태완(카네비모빌리티)

2024년 11월 28일 (목)

세션	논문번호	논문제목(저자)
11:00~12:00 (1-4) 해킹과 취약점 분석 1 좌장: 이현우 (KENTECH)	218	분산 시스템 퍼징을 위한 포괄적 네트워크 상태 전이 기반 접근 김원회, Ahmad Elmoursi, 강민석(KAIST)
	41	USB 드라이버 퍼징을 위한 장치 프로토콜 규격의 자동 생성 강민석, 송도경(연세대학교)
	78	동적 컨텍스트 생성 함수 레벨 퍼징 기술을 이용한 실시간 운영체제 취약점 분석 연구 이은규, 박준영, 윤인수(KAIST)
	272	MITRE ATT&CK 기반 침투 테스트 자동화 도구 구현 김승혁, 정재영, 김재석, 윤건우, 서준호, 프라티위 밀라티, 최윤호(부산대학교)
	105	영어 및 한국어 탈옥 완화 템플릿을 활용한 PromptGuard의 탐지 성능 및 실효성 분석 나현식, 박성호(숭실대), 윤두식(이로운앤컴퍼니), 최대선(숭실대)
11:00~12:00 (1-5) IoT/로봇보안 좌장: 이재승 (NSR)	139	IoT 환경을 위한 암시적 인증서 기반 KEM-TLS 한윤선, 서석충(국민대학교)
	203	소형 상용 드론에 대한 사이버 공격 연구 동향 분석 정희성, 김형식(성균관대학교)
	240	멀티 로봇 시스템을 위한 블록체인 기반 리더 로봇 선정 모델 설계 이수진,서승현(한양대학교)
	52	RolFuzz: 강화된 로봇 보안 정책을 적용한 ROS IDL 퍼저 연구 박민건, 유지현, 윤주범(세종대학교)
11:00~12:00 (1-6) 제로 트러스트/ 네트워크 보안 좌장: 이일구 (성신여대)	4	물리보안 시스템을 위한 제로 트러스트 아키텍처 프레임워크 주진국, 김민재(호텔롯데 롯데월드), 이일구(성신여자대학교)
	232	클라우드 환경에서의 제로트러스트 한계 분석 김미연, 최상훈, 박기웅(세종대학교)
	113	제로트러스트 도입을 위한 소프트웨어 정의 경계(SDP) 성능 분석 모델: 큐잉 네트워크 접근법 이승운, 조병모(LIG 넥스원)
	201	O-RAN 환경에서의 제로트러스트 접근제어 모델 제안 목정현, 이석준(가천대학교)
	44	공격 그래프 기반의 사이버 공격 시나리오 모델링 노성현, 김태성(충북대학교)

2024년 11월 28일 (목)

세션	논문번호	논문제목(저자)
13:00~14:00 (2-1) KpqC 좌장: 노동영 (NSR)	194	8KB 칩셋에서의 양자내성암호 적용을 위한 SMAUG-T 메모리 최적화 오원영(Best of the Best), 문경태(한양대학교), 박정식(경희대학교), 권보연(대구가톨릭대학교), 김진영(성균관대학교), 한주성(쿠팡), 윤기순(NSHC)
	149	kpqm4: KpqC 공모전 알고리즘에 대한 ARM Cortex-M4 벤치마킹 프레임워크 최용렬, 서석충(국민대학교)
	35	라즈베리파이 5 상에서의 KpqC 2라운드 성능 비교 윤세영, 심민주, 차상민, 서화정(한성대학교)
	224	KpqC 2라운드 전자서명 NCC-Sign에 대한 상관 전력 분석 조홍래, 한재승, 한동국(국민대학교)
	237	부호 기반 키 체결 PALOMA의 성능 측정에 관한 연구 이제원, 김동현, 박동현, 김민지, 김동찬(국민대학교)
13:00~14:00 (2-2) 인공지능과 보안 II 좌장: 심규석 (KISTI)	151	대규모 언어모델 한국어 탈옥 프롬프트 분류기 연구 박대얼, 장현준(숭실대학교), 윤두식(이로운앤컴퍼니), 최대선(숭실대학교)
	53	잠재 확산 모델을 활용한 오디오 생성에서의 데이터 복제 메커니즘 김보나, 조민지, 오세은(이화여자대학교)
	73	격차 기반 적대적 훈련을 통한 인증 가능한 강건성 정확도 개선 백진현, 심상훈, 최원석(고려대학교)
	45	이미지 데이터 비식별 수준에 따른 보상체계 함수 추정 최유정, 김태성(충북대학교)
	198	CNN 분류기를 통한 적대적 공격 필터링 및 보호 안드로 아프릴라 아디푸트라, 황연정, 레티투흐엉, 김호원(부산대학교)
13:00~14:00 (2-3) 모빌리티 보안 II 좌장: 이원혁 (KISTI)	7	차량 임베디드 시스템을 위한 사이버보안 로깅 시스템 구축 이지우, 이현빈, 이준택(한국자동차연구원)
	135	자율 주행 차량의 차선 인식 알고리즘에 대한 적외선 활용 공격 기술 제안 주현민, 우상민, 김도현, 최원지, 김재훈, 김용대(KAIST)
	146	차량 네트워크의 비정상 행위 탐지를 위한 LSTM-PacGAN 모델 이민종, 김수형, 하재철(호서대학교)
	2	V2X 메시지 기반의 지속적인 이상행위 차량 식별을 위한 추적 기법 이지우, 김찬민, 이준택, 권민희(한국자동차연구원)
	21	CAN 네트워크 보안 위협 분석과 완화를 위한 룰 기반 침입 탐지 기법에 관한 연구 오형석, 조성현(한국자동차연구원)

2024년 11월 28일 (목)

세션	논문번호	논문제목(저자)
13:00~14:00 (2-4) 해킹과 취약점 분석 II 좌장: 박기웅 (세종대)	83	Matter 프로토콜 보안 메커니즘 및 취약점 분석 연구 김서연(순천향대학교), 권순범(고려대학교), 금성(건양대학교), 박동혁(서울과학기술대학교), 성준우(영남이공대학교), 김채원
	67	계측 콜백 기반 권한 상승 탐지 송희원, 강성우, 김택우, 심수민, 양준헌, 이승대(KITRI BEST OF THE BEST), 김동준(엔키 화이트햇), 전상현(악성코드검거단)
	162	메타모픽 테스트를 활용한 NIST PQC Additional Round 2 전자서명 알고리즘 구현 취약점 분석 신동현, 김영범, 서석충(국민대학교)
	163	MLP에 대한 클럭 글리치 기반 오류 주입 영향 분석 강효주, 홍성우, 김윤성, 하재철(호서대학교)
	37	CodeQL Taint Analysis를 활용한 SBOM 탐지 취약점의 실질적인 위협 선별 기술 제안 정윤영(성신여자대학교), 유승준(중앙대학교), 김수연(성신여자대학교), 김수현(중부대학교), 안세은(수원대학교), 장현진(부산대학교), 임원빈(스틸리언), 김두민(SK텔레콤), 문광석(코리안리)
13:00~14:00 (2-5) 암호이론과 구현 I 좌장: 구본욱 (NSR)	104	AES 기반 AEAD 스킴의 키 커밋 공격 복잡도 계산 김선규, 신명수, 신한범, 김인성, 김선엽, 권동근, 석병진, 이동재(강원대학교), 홍득조(전북대학교), 성재철(서울시립대학교), 홍석희(고려대학교)
	133	축소 라운드 LEA에 대한 새로운 선형 구별자 신명수, 김선규, 신한범, 김인성, 김선엽, 권동근, 석병진(고려대학교), 이동재(강원대학교), 홍득조(전북대학교), 성재철(서울시립대학교), 홍석희(고려대학교)
	134	부분합 기법과 FFT 기법을 활용한 6-라운드 AES에 대한 새로운 Square 공격 신한범, 김선규, 신명수, 김인성, 김선엽, 권동근, 석병진(고려대학교), 이동재(강원대학교), 홍득조(전북대학교), 성재철(서울시립대학교), 홍석희(고려대학교)
	268	증명 가능한 안전성을 지닌 고속 AES S-Box 고차 마스킹 안현준, 한동국(국민대학교)
	205	ARADI 암호의 바이트 동일 특성 김선엽, 김선규, 신명수, 김인성, 신한범, 권동근, 석병진(고려대학교), 이동재(강원대학교), 홍득조(전북대학교), 성재철(서울시립대학교), 홍석희(고려대학교)

2024년 11월 28일 (목)		
세션	논문번호	논문제목(저자)
13:00~14:00 (2-6) 금융보안/ 정보보호 정책, 법, 제도 좌장: 유지현 (광운대)	261	NIST SP 800-53 Rev. 4에 기반한 K-RMF 특성 비교 양우열, 이윤경, 이상민, 김영세(한국전자통신연구원)
	215	한·미 사이버범죄 대응정책 비교분석 및 강화방안 -국가사이버안보전략을 중심으로- 이경주(한국저작권보호원), 김기범(성균관대학교)
	202	국내은행 고객 데이터 기반 선불전자지급수단 사칭범죄 탐지 연구 이혜림, 오중산(숙명여자대학교)
	49	사이버 복원력 측정을 위한 평가 지표 구성에 관한 연구 이새움, 최슬기, 김태현, 오동환, 임준형, 김태은(한국인터넷진흥원)
	40	러시아-우크라이나 사이버전 사례를 통한 사이버전 훈련 시나리오 연구 김대운, 나사랑, 박성민, 임준형(한국인터넷진흥원)

2024년 11월 28일 (목)

세션	논문번호	논문제목(저자)
14:10~15:10 (3-1) 양자보안 II 좌장: 임재덕 (ETRI)	197	쇼어 알고리즘 최적화를 위한 양자 회로에서의 연산 알고리즘 구현 조재한, 신다윗, 김호원(부산대학교)
	231	Gao-Mateer Additive FFT의 반복문 방식 구현에 관한 연구 박동현, 김민지, 이제원, 김동현, 김동찬(국민대학교)
	82	Toom-Cook 기반 곱셈기의 점근적 성능 분석 리니 위누스 와르다니, 데디 셉토노 차투르 푸트란토, 조재한, 신다윗, 김호원(부산대학교)
	252	V2X 환경에서 CBOR 인코딩을 활용한 Partial Hybrid 인증서 사이즈 최적화 연구 강정훈, 서승현(한양대학교)
	249	임베디드 환경에서의 PQC 인증서 전송 오버헤드 분석 김제인, 서승현(한양대학교)
14:10~15:10 (3-2) 인공지능과 보안 III 좌장: 진승헌 (ETRI)	253	공격적 보안을 위한 언어 모델 평가: 침투 테스트 응용을 위한 벤치마크 및 메트릭 조사 수랸토 나우팔, 데리 프라타마, 신다윗, 김호원(부산대학교)
	229	FlowCluster: 네트워크 플로우 데이터셋 군집화 연구 이윤호, 최유나, 김현민, 조항범, 윤명근(국민대학교)
	188	LCNN 기반 딥보이스 탐지기에 대한 적대적 공격 이영주, 홍성우, 하재철(호서대학교)
	16	스마트 컨트랙트 취약점 탐지를 위한 LLM 적용 방안 연구 박상욱, 이범수, 김호원(부산대학교)
	25	로그 기반 이상 탐지용 심층학습 모델 최근 연구 동향 이수연, 구형준(성균관대학교)
14:10~15:10 (3-3) 모바일 보안/ 소프트웨어 보안 좌장: 한상윤 (NSR)	243	Analysis of Dynamic Testing Approaches for Application Security in Mobile Environment 가드가 넘러타, 레리사 아데바 질차, 김득훈, 곽진(아주대학교)
	61	LLM 기반 모바일 앱 시나리오 테스트 기술 동향 나보림, 이승민, 조효진(연세대학교)
	155	Drone Arm 프로세서 디버깅 및 트레이싱 모듈의 심층 탐구와 활용 하태욱, 장진수(충남대학교)
	263	Linux OS 대상 랜섬웨어 탐지 기법 동향 최재민, 최상훈, 박기웅(세종대학교)
	192	리눅스 기반 런타임 타입 SBOM 생성 방법과 구현 손현승, 김지민, 이만희(한남대학교)

2024년 11월 28일 (목)

세션	논문번호	논문제목(저자)
14:10~15:10 (3-4) 네트워크보안 좌장: 서화정 (한성대)	225	뿌리공정 네트워크 트래픽에 대한 E2E 암호화와 TLS 기반 암호화의 성능 비교 분석 황연정, 강은세, 익발 무함마드, 김호원(부산대학교)
	76	무선통신 환경에서의 데이터 은폐 기법과 은닉 채널 형성 방법 조사 박지훈, 최상훈, 박기웅(세종대학교)
	13	외부 참여자가 다자간 데이터 교집합을 계산하는 MPSI 프로토콜에 관한 연구 김기환, 윤성철, 김수현, 이임영(순천향대학교)
	152	악의적 단말 기반 이동통신 코어 네트워크 보안 테스트 김광민, 손민철, 오범석, 김덕우(KAIST), 박철준(경희대학교), 김용대(KAIST)
14:10~15:10 (3-5) 디지털 포렌식/ 취약점 분석 1 좌장: 장상운 (NSR)	131	비 설치형 인스턴트 메신저 네이버톡에 대한 디지털 포렌식 관점에서의 데이터 수집 연구 위다빈, 김한결, 안원석, 박명서(한성대학교)
	5	드론 포렌식 도구 검증 방법론 기초 연구 이상철, 이철한, 윤우성, 박정흠(고려대학교)
	251	디지털포렌식 관점의 기술유출 동향 분석 및 향후 연구 제안 이정인, 김준기, 박정흠(고려대학교)
	193	위협모델링 프레임워크 기반 위협원 위험평가 방안 송유래, 김득훈(아주대학교), 안상현(국군방첩사령부), 곽진(아주대학교)
	244	위성 통신 시스템에 대한 보안 취약점 및 대응 방안 이한, 전희도, 최원석(고려대학교)
14:10~15:10 (3-6) 기업 소개 및 채용상담 좌장: 이태진 (호서대)		정보보호관련 기업 소개 및 채용상담 LIG넥스원, 현대모비스

2024년 11월 29일 (금)

세션	논문번호	논문제목(저자)
9:30~10:30 (4-1) 양자보안 III 좌장: 석우진 (KISTI)	72	AVX2와 VPCLMULQDQ 명령어를 활용한 HQC의 GF(2)[x] 다항식 곱셈 최적화 장지훈, 이명훈(고려대학교), 김수리(성신여자대학교), 홍석희(고려대학교)
	148	NCC-Sign HW Modular Multiplication 구현 방안 연구 김영범, 서석충(국민대학교)
	156	SMAUG-T 다항식 곱셈 최적화 방안 연구 고우형, 김영범, 서석충(국민대학교)
	154	Cortex-M4에서의 Falcon 부동 소수점 연산 개선 방안 분석 연구 최준혁, 서석충(국민대학교)
	222	NIST PQC 표준화 알고리즘 연구 및 전환 동향 정병욱, 강은세, 황연정, 김호원(부산대학교)
9:30~10:30 (4-2) 인공지능과 보안 IV 좌장: 김수현 (순천향대)	20	인공신경망 구조를 활용한 사이버보안 복원력 평가 지표체계 및 평가방법론에 대한 연구 오동완, 이새움, 최슬기, 김태현, 김태은(한국인터넷진흥원), 곽진(아주대학교)
	204	Log Dataset Distributional Variability and its Implication for Robust Log Anomaly Detection 레리사 아데바 질차, 김득훈, 곽진(아주대학교)
	63	Trajectory backdoor Detection: NIDS환경에서의 Transformer Attention Score를 활용한 백도어 공격 탐지 제안 장진혁, 박소희, 최대선(숭실대학교)
	43	MALCL: GAN 기반 Generative Replay를 활용하여 Malware 분류의 Catastrophic Forgetting을 해결 박지민, 박민지, 지아현, 오세은(이화여자대학교), Mohammad Saidur Rahman(The University of Texas at El Paso)
	270	모아레 패턴이 딥페이크 탐지 성능에 미치는 영향 허민지, Razaib Tariq, 우사이먼성일(성균관대학교)
9:30~10:30 (4-3) 블록체인 보안 좌장: 이만희 (한남대)	255	전기차 배터리 데이터의 신뢰성 검증을 위한 배터리 관리 시스템(BMS)용 블록체인 플랫폼 설계 김재현, 김호원(부산대학교)
	230	양자 내성 블록체인 동향 김현준, 서화정(한성대학교)
	84	블록체인 환경에서 안전하고 신뢰 가능한 키 백업 및 복원 프로토콜 신수진, 박예현, 신상욱(부경대학교)
	12	검증 가능한 검색 가능 암호화와 스마트 컨트랙트 김예은, 오희국(한양대학교)
	266	블록체인과 속성 기반 프록시 재암호화를 활용한 의료 데이터 프라이버시 보호 모델 제안 정은혜, 이경현(국립부경대학교)

2024년 11월 29일 (금)

세션	논문번호	논문제목(저자)
9:30~10:30 (4-4) 산업보안/ 모바일보안 좌장: 박정수 (강남대)	271	생성형 AI KoBERT 모델을 활용한 융합안전 질의 응답 시스템 개발 배종옥, 임준묵(한밭대학교)
	143	산업제어시스템의 침해사고 대응을 위한 Sysmac Studio 아티팩트 분석 신지호, 김기범(성균관대학교)
	102	ICS 데이터를 활용하는 설명가능한 멀티모달 기반 단계적 사이버 공격 탐지 모델 제안 이주현, 전승호, 서정택(가천대학교)
	184	ICS 인프라 데이터 셋을 활용한 머신러닝 학습 및 이상 징후 탐지 연구 박성태, 백찬영(SK 쉴더스, KG에듀원아이티뱅크)
9:30~10:30 (4-5) 웹 서비스 보안 좌장: 김득훈 (아주대)	166	다크웹 연구 동향과 향후 연구 방향에 대한 고찰 김도희, 황성재(성균관대학교)
	55	슬랙 협업 서비스를 활용한 기술유출 행위 추적 기법 연구 오지웅, 김준기, 박정흠(고려대학교)
	56	Works Drive 협업용 클라우드 스토리지에 대한 데이터 수집 및 사용자 행위 분석 연구 김한결, 위다빈, 안원석, 박명서(한성대학교)
	90	YouTube에서의 은닉 스팸 탐지: RAG와 LangChain 프레임워크를 활용한 관계 기반 접근 기법 이범수, 윤지원, 레티투흐엉, 김호원(부산대학교)
	10	SOAR 기반 보안 관제 업무 효율성 향상을 위한 플레이북 자동 생성 시스템 최슬기, 이새움, 김태현, 오동환, 임준형, 김태은(한국인터넷진흥원)

2024년 11월 29일 (금)

세션	논문번호	논문제목(저자)
10:40~11:40 (5-1) 하드웨어 보안 좌장: 서석충 (국민대)	199	CycloneDX HBOM을 통한 하드웨어 취약점 관리 방안 김지민(한남대학교), 김문선(소프트버스), 이만희(한남대학교)
	81	무기체계 적용을 위한 안티탬퍼 하드웨어 연구동향 최준호, 이규호(LIG Nex1)
	86	컨테이너 환경에서의 RDMA NIC 마이크로아키텍처 자원 고갈 영향 분석 김건우, 김진우, 박병준(광운대학교)
	157	GPU 상에서의 이진 필드 다항식 곱셈 최적화 김동천, 서석충(국민대학교)
	103	임베디드 기기의 암호화된 펌웨어 이미지 복호화 기법 연구 이철한, 정수은, 박정흠(고려대학교)
10:40~11:40 (5-2) 부채널 보안 I 좌장: 심보연 (ETRI)	258	드론 대상 전자파 오류 주입 공격에 대한 선행 연구 박혜진, 한동국(국민대학교)
	181	멀티콥터의 PWM 통신 채널에 대한 EMI 신호 주입 공격 기법 연구 김의진, 조현수, 이지원, 최원석(고려대학교)
	66	부채널 분석 기반 하드웨어 트로이목마 탐지 연구 동향 박수진, 배대현, 이정환, 김희석, 홍석희(고려대학교)
	189	전자기파 기반 공격 기법 연구 동향 최지훈, 이지원, 조현수, 최원석(고려대학교)
	145	DNN 모델 보호를 위한 전적 분할되고 효율적인 인스트럭션 추적 기반 모니터링 하드웨어 송용호, 우병수, 한영광, 강병훈(KAIST)
10:40~11:40 (5-3) 인공지능 / 기타 정보보안 좌장: 박소희 (ETRI)	168	머신 언러닝의 메트릭에 대한 조사 김준형, 황성재(성균관대학교)
	33	Grad-CAM을 이용한 딥페이크 음성 탐지 시스템의 결정 설명 이웅재, 홍기훈, 정수환(숭실대학교)
	121	DisplayLink와 호환되는 USB 장치의 구현 김지율, 김창훈(대구대학교)
	23	Advanced Persistent Threats: Addressed and Open Research Questions Shakhzod Yuldoshkhujaev, 구형준(성균관대학교)
	60	IoT 장치 인증 프로토콜을 적용한 안전한 유통망 모델 박예현, 신수진, 신상욱(부경대학교)

2024년 11월 29일 (금)

세션	논문번호	논문제목(저자)
10:40~11:40 (5-4) 공급망 보안 좌장: 박명서 (한성대)	269	군용 인공지능을 위한 디지털 서명 기반 공급망 보안 체계 구축 방안 장예준, 김록기, 이영화(육군미래혁신연구센터)
	177	원자력시설 컴퓨터 및 정보시스템 보안 규정의 공급망 보안 요구사항 분석 정윤정, 이준희, 이만희(한남대학교)
	161	OT 시스템 운영자 관점의 공급망 보안 요구사항 연구 이준희, 정윤정, 이만희(한남대학교)
	178	IEC 62433 기반 개발자를 위한 OT 공급망 보안 요구 사항 연구 정윤정, 이준희, 이만희(한남대학교)
	24	인공위성 공급망 보안 강화를 위한 소프트웨어 기반 아이디어 연구 연동현, 장대희(경희대학교)
10:40~11:40 (5-5) 공공 인프라 보안 좌장: 이새움 (KISA)	18	공공기관 조직구성원의 정보보안행동에 미치는 영향요인에 관한 연구 이영철, 장길상(울산대학교)
	101	원자력시설 대상 사이버사건대응 체계 및 역량 평가 방안 제시 최희원, 이주현, 전승호, 서정택(가천대학교)
	88	Anomaly Detection in Nuclear Power Plant 아비섹 차우드하리, 한준서, 김성아, 최선오(전북대학교)
	158	5G 통신 환경에서의 기지국 인증 기반 허위 기지국 탐지 동향 분석 김민기, 한윤선, 김영범, 서석충(국민대학교)
	209	CCS 기반 전기차 충전 시스템에 대한 은밀한 서비스 거부(DoS) 공격 박유희, 김주언, 최원석(고려대학교)

2024년 11월 29일 (금)

세션	논문번호	논문제목(저자)
13:00~14:00 (6-1) 개인정보보호 좌장: 김소정 (INSS)	127	추적 가능한 프라이버시 강화 CBDC 설계 동향 분석 이예지, 정익래(고려대학교)
	11	전화/문자 발신번호 유효성 확인서비스 모델 박해룡, 석지희, 김진리, 오진영(한국인터넷진흥원)
	264	알고리즘 삭제명령 도입에 관한 연구 주지연, 김기범(성균관대학교)
	30	메모리 분석을 통한 데이터베이스 정보유출 위험성에 대한 연구 오상원(에이치엠컴퍼니), 서종찬(청주대학교), 손석훈(서원대학교),우현우(대구가톨릭대), 이덕규(서원대학교)
	130	표준 분석을 통한 AI 개인정보보호 자율점검표 개정 검토 박진용, 박병조, 김태성(충북대학교)
13:00~14:00 (6-2) 부채널 보안 II 좌장: 김은영 (LIGNEX1)	238	전력과 전자파 기반 준침입 공격: 효과적인 오류주입을 위한 도구 임성혁(국군방첩사령부), 지재덕, 한동국(국민대학교)
	170	고사양 장비에 대한 상관 전자파 분석. 김주환, 한동국(국민대학교)
	79	Windows 환경에서 Intel RAPL DRAM 도메인을 통한 캐시 부채널 분석 최민식, 김희석, 홍석희(고려대학교)
	140	결합 확률 분포 기반 부채널 분석 기법에 대한 연구 이인훈, 김희석, 홍석희(고려대학교)
	70	ENF 신호 기반 음원 위치 추정을 위한 공간 보간 기법 비교 분석 한혜경, 안효진, 윤상범(LIG 넥스원)
13:00~14:00 (6-3) 시스템 보안 좌장: 박철준 (경희대)	39	OSS 검출의 정확성 향상을 위한 경로 정보 활용 이준규, 임종환(스패로우)
	175	효율적인 APT 시뮬레이터 프레임워크 제안 허남정, 최상훈, 박기웅(세종대학교)
	213	타이포스쿼팅 공격 및 탐지 연구 동향 방수경, 김형식(성균관대학교)
	26	검색 증강 생성 (RAG) 시스템 공격과 방어 연구 동향 김민석, 구형준(성균관대학교)
	85	HarassWatch: 소셜 VR 플랫폼에서의 피해자 관점 괴롭힘 행위 탐지 이준희, 김진우(광운대학교)

2024년 11월 29일 (금)

세션	논문번호	논문제목(저자)
13:00~14:00 (6-4) 학부생 우수 논문 좌장: 전상훈 (국민대)	31	최신 ASV 적대적 공격의 문제점 고찰 및 개선방안 제안 이요원, 홍기훈, 정수환(숭실대학교)
	196	차분 및 선형 공격에 대응을 위한 경량 암호 MGFN의 필요 라운드 수 분석 김남일, 송원우, 전용진, 백승준, 김종성(국민대학교)
	245	차세대 Military-BcN 5G 상용망 연동 시 모바일 업무 환경 보안 기법 연구 김찬혁 , 김형엽 , 위한샘 , 이옥연(국민대학교)
	250	KpqC 2라운드 후보 TiMER의 메시지 인코딩에 대한 단일파형공격 유성환, 한재승, 한동국(국민대학교)
	257	불법 콘텐츠 배포 방지를 위한 CNN 기반 딥 페이크 탐지 기술 조경수 , 문지윤 , 오준희 , 이종혁(세종대학교)
13:00~14:00 (6-5) 디지털 포렌식/ 취약점 분석 2 좌장: 김종성 (국민대)	111	딥러닝 기반 디지털 성범죄물 탐색 모델 성능 평가 하영정, 신승운, 박지호, 김승현, 권태경(연세대학교)
	115	한국어 딥보이스 판별을 위한 다중 딥러닝 모델 비교 연구 이치훈, 김영록, 김병관, 김수진, 권태경(연세대학교)
	110	범죄에 이용된 해외 가상자산 거래의 연관성 분석 모델 설계 이해찬, 전유등, 장연주, 김선진, 권태경(연세대학교)
	160	사이버범죄를 통한 비대면인증 취약점 분석 및 웨어러블 기기 기반 개선 방안 송현중, 장우성, 최경수, 조효진, 권태경(연세대학교)
	109	적대적 공격에 대한 딥페이크 탐지 모델의 강건성 분석 김영수, 박대형, 윤병선, 민상규, 이재희, 권태경(연세대학교)

2024년 11월 28일 (목)

세션	논문번호	제목(저자)
11:00~12:00 포스터 1 좌장: 김효승 (한림대)	179	사이버 복원력 정량적 평가지표 제시 강혜진, 성지현, 조학수(호서대학교)
	180	임의의 픽셀 단위 섭동에 대한 컴퓨터 비전 모델의 강건성 분석 연구 이정엽, 김아연, 박래현, 권태경(연세대학교)
	183	AI 포렌식을 위한 XAI 기반 기술과 법적 신뢰성 확보 방안 권순신, 한상수, 권태경(연세대학교)
	185	최신 퍼징 분야에서의 LLM 활용 동향 김태호, 정지우, 권태경(연세대학교)
	187	로봇 네트워크에서 블록체인 기반 데이터 공유 모델 동향 이고은, 홍다희, 서승현(한양대학교)
	97	물리적 복제 방지 함수(PUF)의 안정성 향상을 위한 비트 오류율 감소 기술 분석 이지은, 김태호(서울여자대학교), 임재덕(한국전자통신연구원)
	195	랜섬웨어 복호화 도구 개발 동향: XOR 특성을 활용한 복호화 사례를 중심으로 조동후, 박진철, 박지수, 박세준, 강수진, 김종성(국민대학교)
	206	클라우드 보안 위협에 대응 가능한 SOAR 프레임워크 이승현(성신여자대학교), 하진우(건국대학교), 윤태호(수원대학교), 이한선, 임영서(이화여자대학교)
	207	비콘 인터벌 변조를 활용한 에어 갭 네트워크의 정보 유출 공격 정예림, 김소연, 이일구(성신여자대학교)
	210	머신러닝 모델 추출 공격 방어를 위한 접근법 분류 권석재, 이세영(강원대학교)
	211	Storm Chaser: O-RAN에서 Signaling Storm DoS를 차단하는 eBPF/XDP 기반 보안 프레임워크 김현문, 이승수(인천대학교)
	214	기계학습 디컴파일러 학습 개선을 위한 의사코드 전처리 방안 이정호, 이세영(강원대학교)
	216	국내외(NIST, KpqC 연구단) 양자내성암호 동향 임진한, 윤혜진, 이옥연(국민대학교)
	217	ROS 기반 로봇 통신의 신뢰성 향상을 위한 연구 동향 조사 박가을, 서승현(한양대학교)
	208	글로벌 DDoS 공격 동향 분석 및 대응방안 이재형, 김득훈, 곽진(아주대학교)
	221	VRMask: 소셜 VR 플랫폼의 유해 컨텐츠 탐지 및 마스킹 김종섭, 김동은, 김진우(광운대학교)
	223	FaaSMon: 프로비넌스 GNN 기반 서버리스 침입 탐지 시스템 정지환, 양정용, 이혜진, 김진우(광운대학교)

2024년 11월 28일 (목)

세션	논문번호	제목(저자)
11:00~12:00 포스터 1 좌장: 김효승 (한림대)	227	산업제어시스템에서의 OPC UA 취약점 유형 분석 및 대응 방안 연구 이수미, 장지인, 고승현, 오현수, 이종엽, 양정규, 한철규(KITRI Best Of the Best)
	228	로봇 시스템 모니터링 연구 동향 지찬웅, 박가을, 이수진, 서승현(한양대학교)
	94	사이드카 인젝션 공격: 쿠버네티스 환경에서 Mutating Webhook 악용 조치현, 이승수(인천대학교)
	236	V2X 환경에서의 네트워크 보안 위협과 영향 분석 안선영, 전상훈(국민대학교)
	239	네트워크 행위에 대한 특징 분석 및 공격유형 해석방안 연구 박현우, 이주영, 정혜란, 서유민, 김현서, 이태진(호서대학교)
	241	AFF4-L과 ECo-Bag 기반 선별 수집 및 증거 관리를 위한 논리 이미지 포맷 개발 김경민, 임소린, 정수은, 박정흠(고려대학교)
	247	블록암호 GIFT-128의 난수성 분석 이명규, 성재철, 홍석희(고려대학교)
	248	VoLTE의 SIP 프로토콜 취약점 분석 환경 및 연구 동향 분석 최현영, 박철준(경희대학교)
	254	이동통신망에서 무선 구간 공격자 무력화를 위한 resource depletion 취약점 연구 공태현, 박철준(경희대학교)
	256	안전한 로봇 운영 시스템에 관한 연구 강신호, 서지원(단국대학교)
	259	5G 슬라이싱 보안 취약점 연구 동향 분석 민수림, 김환국(국민대학교)
	260	ApriSig: A-priori 알고리즘 활용 데이터 기반 침입 탐지용 서명 자동 생성 프레임워크 박서현, 황명하, 권유진, 이현우(한국에너지공과대학교)
	262	통신환경의 전송 속도를 고려한 KpqC 라운드 2 알고리즘의 성능 분석 김제빈(서울시립대학교), 장지훈, 이명훈(고려대학교), 김수리(성신여자대학교), 성재철(서울시립대학교), 홍석희(고려대학교)
	265	가상자산 관련 범죄수사를 위한 온오프라인 데이터 연계 방안 이승은, 한민선, 김보송, 강윤진, 이진민, 이일구(성신여자대학교)
	267	연속된 MCT 게이트 회로에서 Toffoli의 전략적 큐비트 선택을 통한 Depth 감소 오진섭, 최찬호, 최두호(고려대학교)
	220	CyberSecurity Incident Investigation Tool 김태윤, 김가영, 배기태, 서주형, 김찬형, 윤종희(영남대학교)
	22	SOAR 를 위한 Generative AI 활용방안 민천호, 김득훈, 곽진(아주대학교)

2024년 11월 28일 (목)

세션	논문번호	제목(저자)
13:00~14:00 포스터 2 좌장: 곽병일 (한림대)	98	로그 크기의 CRS를 갖는 양자내성 PAKE 프로토콜 구성 김현서, 이예솔, 황정연(성신여자대학교)
	99	해양 환경에서의 GNSS 대상 공격 탐지기법 연구 동향 분석 임호진, 고아름, 이주현, 서정택(가천대학교)
	100	자율주행 로봇의 LTE 기반 전화 송신 프라이버시 위협 분석 연구 김채영, 박민영, 한아림, 이진, 이훈희, 허준원, 김찬인(KITRI Best of the Best), 이창선(상명대학교), 김경곤(나이프아랍안보과학대)
	106	AutoCANFuzz: 실차 환경에서의 자동화된 퍼징 프레임워크 최정민, 전상훈(국민대학교)
	108	APT 공격 시나리오를 통한 AD 환경에서의 기만 기술 적용 연구 박윤진, 김세연, 김성욱(서울여자대학교)
	112	클라우드 환경에서의 제로 트러스트 구현을 위한 SASE 기술 활용 사례 연구 이주현, 최원휘, 박정수(강남대학교)
	117	AI 모델 보안성 확보를 위한 RMF 설계 및 적용 방안 한상수, 권태경(연세대학교)
	118	광학신호 기반 은닉 채널 기술 분석 이정민, 손우영, 권순홍, 이종혁(세종대학교)
	119	IoT 환경에서 머신러닝과 SDP 통합을 통한 동적 보안 기법 김현지, 김민지, 장유정, 박후린(서울여자대학교)
	120	Retrieval-Augmented Generation 시스템의 구조적 취약성 및 공격 벡터 분석 이지혜, 이연재, 강충현, 김경국, 권영훈, 이태관, 박의성(KITRI Best of the Best)
	122	CLIP 모델 미세 조정을 통한 제로샷 기반 딥페이크 탐지 성능 향상 연구 이재희, 권태경(연세대학교)
	124	생성형 모델의 악의적 위협에 대응하기 위한 가드레일 방어 기술 분석 연구 김아연, 이정엽, 박래현, 권태경(연세대학교)
	125	Chirp 분석을 통한 LoRa Jamming 공격신호 복구 기법 김성훈, 전희도, 최원석(고려대학교)
	126	대규모 언어 모델의 최신 Jailbreak 기법, 성공 평가 및 통합 프레임워크 분석 조주원, 안홍은, 박래현, 권태경(연세대학교)
	128	비정규 인터페이스 기반 EDR 데이터 획득 기술 제안 이동원, 김성현, 유수연, 함동찬, 우사무엘(단국대학교)
	129	새로운 순열을 활용한 PRESENT 블록암호 최적화 구현 백지우(성신여자대학교), 신명수, 신한범, 홍석희(고려대학교)
	132	소프트웨어 공급망 보안에 관한 조사 김영석, 황성재(성균관대학교)

2024년 11월 28일 (목)

세션	논문번호	제목(저자)
13:00~14:00 포스터 2 좌장: 곽병일 (한림대)	136	스마트폰 무음 파일 재생을 이용한 전자파 은닉 채널 김용재, 안현준, 한동국(국민대학교)
	137	생성형 AI 의 개인정보 수집에 대한 국제 규제 비교 및 정책 제안: 국내 금융권의 생성형 AI 도입 규제 개선을 중점으로 서다인(서울여자대학교), 이가현(조선대학교), 김다희(고려대학교), 이지수(가천대학교), 안가은(서울여자대학교)
	138	안드로이드 환경에서의 다음 카페 어플리케이션 로컬 아티팩트 분석 및 활용 연구 안원석, 박명서(한성대학교)
	141	IQPnC: Implicit Quantum Plug and Charge V2G 통신에서 효율적인 양자내성암호 전환 연구 강성민, 한윤선, 서석충(국민대학교)
	142	MacOS 취약점 탐지 동향에 관한 연구 정지우, 권태경(연세대학교)
	144	NIST PQC HW/SW 공동 설계 동향조사 이재석, 김영범, 서석충(국민대학교)
	147	일반화 데이터셋 구축을 위한 딥페이크 생성기법 동향 분석 김현준, 권태경(연세대학교)
	150	기호 실행을 통한 블록 암호의 구현 정확성 검증 지용현, 김영범, 서석충(국민대학교)
	153	RISC-V 환경에서 블록 암호 HIGHT 최적 구현 김채린, 최용렬, 서석충(국민대학교)
	159	경량 IoT를 위한 규칙 기반 고효율 병렬 퍼징 프레임워크 신주영(중앙대학교), 김연진, 박나은, 이일구(성신여자대학교)
	164	LLM 및 MLLM을 대상으로 한 탈옥 공격 분석: 공격 턴 수와 모달리티 기반 접근 안홍은, 조주원, 권태경(연세대학교)
	93	인공 지능 기반 딥보이스 생성 방어를 위한 음성 재구성 방안 연구 김승민, 박소희, 최대선(숭실대학교)
	167	안드로이드 환경에서 모임 애플리케이션 소모임의 암호화된 채팅 내역 복호화 연구 이용진, 김강한, 신관용, 박세진, 강수진, 김종성(국민대학교)
	169	디지털 포렌식 관점에서의 동호회 애플리케이션 아티팩트 분석 박진철, 안현종, 김현준, 박지수, 강수진, 김종성(국민대학교)
	96	컨테이너 이미지 취약점 스캐닝 기술 연구 동향 오채린(공주대학교), 김현일(조선대학교), 홍도원, 서창호(공주대학교)
	174	정보주체 권리 통합과 보안성 강화를 위한 중앙집중식 마이페이지 시스템 제안 장한나(성신여자대학교), 박현재(아주대학교), 최승용(청주대학교), 전명환(인하대학교), 전해준(충남대학교), 지한별, 권현준(KITRI Best of Best), 최현우(성신여자대학교)
	176	국내외 디지털 지갑 보안성과 편의성 비교 분석 김경회, 이세영(강원대학교)

2024년 11월 28일 (목)

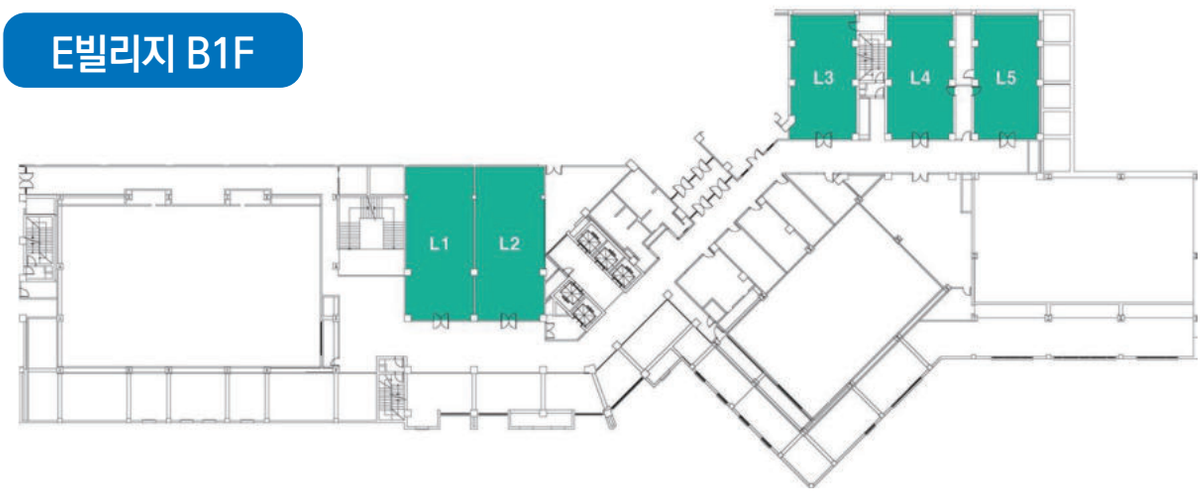
세션	논문번호	제목(저자)
14:00~15:00 포스터 3 좌장: 한미란 (고려대)	172	AI 포렌식의 신뢰성과 투명성 확보를 위한 블록체인 기술 활용 방안 조원영, 김윤식, 권태경(연세대학교)
	3	하드웨어 센서 정보를 이용한 안드로이드 에뮬레이터 탐지 기법 김준호, 김선정, 곽병일(한림대학교)
	8	저사양 환경에서 eBPF/XDP 기술을 이용한 DDoS 공격 대응 방안 함준형, 라민우, 김도현, 강성원, 임정훈, 최홍석, 지도환(한국정보기술원 화이트햇스쿨 2기), 이민우(한국해양대학교)
	9	프로그램의 코드 실행 흐름 추적을 통한 탐지 우회 외부 API 식별 기법 이창민, 한미란, 김준섭(고려대학교)
	14	CCSDS 프로토콜을 통한 인공위성 통신 보안 위협 분석: NOS3 시뮬레이터를 활용한 사례 연구 황선혁, 장대희(경희대학교)
	15	윈도우 환경에서 메모리 포렌식을 통한 카카오톡 데이터베이스 복호화 방안 연구 김민서(성공회대), 조수현(국가보안기술연구소), 김준범(화이트햇 스쿨)
	17	대규모 언어 모델(LLM)을 이용한 국내 정보보호 관리체계(ISMS) 인증심사 GAP 분석 솔루션 개발 진현준(세종대학교), 신우빈(울산대학교), 이동수(수원대학교), 조용권(영산대학교), 최정원(서울여자대학교), 홍영창(소속없음), 송재승(세종대학교)
	27	eBPF와 LDAP 기반 컨테이너 런타임 환경에서의 보안 아키텍처 제안 임학수(명지대학교), 전성현(명지전문대), 정민규(동의대학교), 김현석(조선대학교), 고예준(KAIST), 이창현(단국대학교)
	29	대규모 멀티모달 언어 모델을 활용한 딥페이크 이미지 탐지 연구 장현준, 박성준, 최대선(숭실대학교)
	32	실시간 오디오 딥페이크 탐지 어플리케이션 한성규, 홍기훈, 정수환(숭실대학교)
	34	HAI Dataset을 이용한 최신 이상탐지 모델 성능 비교 한준서, 양호찬, 한윤서, 문서진, 정지현, 김성광(화이트햇 스쿨)
	36	BERTweet 기반의 마약 판매 게시글 탐지 및 PCA를 통한 모델 경량화 이지용(청운대학교), 양승원(건국대학교), 윤동영(가천대학교), 이용균(인하대학교), 이은수(상명대학교)
	38	개인정보보호 관점에서의 중국 전자상거래 앱 보안 취약성 분석 및 평가 정윤영, 김성민(성신여자대학교)
	47	코드 난독화 평가 점수 모델 연구 이지은, 김태호(서울여자대학교), 임재덕(한국전자통신연구원)
	48	CAN data를 활용한 자동차 급발진 탐지에 관한 연구 이정민, 김찬영, 이민호, 곽병일(한림대학교)
	51	클라우드 환경에서의 주요 네트워크 보안 기능 비교 분석 윤석민, 김지수, 남재현(단국대학교)
	58	오픈 소스 대상 AI 기반 퍼징:최신 동향 분석 김재민(세종대학교)
	64	DBC와 머신러닝을 활용한 적응형 하이브리드 CAN IDS 프레임워크 이새나(서울여자대학교), 김송희(아주대학교), 김은지(국민대학교), 박철준(광운대학교), 이재준(아주대학교), 오지훈(대구가톨릭대학교), 전상훈(국민대학교)

2024년 11월 28일 (목)

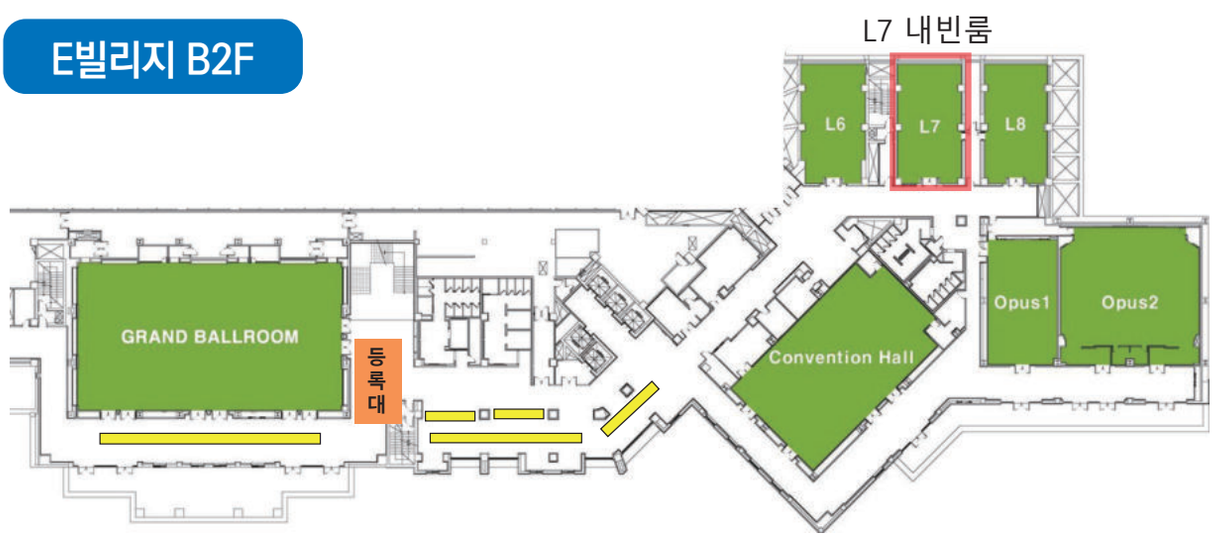
세션	논문번호	제목(저자)
14:00~15:00 포스터 3 좌장: 한미란 (고려대)	68	AI를 활용한 악성 파이썬 패키지 정적 탐지 김동언, 김상구, 신동연, 임수환, 이유식(순천향대학교)
	69	인지과학 기반 대시보드 설계 방안 제시 신윤수(고려사이버대학교), 김도은(학점은행제)
	74	Taint 분석을 사용한 차등적 소스코드 난독화 기법 김남혁(전북대학교), 김상빈(계명대학교), 박하은(가천대학교), 서경호(안동대학교), 조준형(단국대학교)
	75	공급망 보안을 위한 악성 패키지 탐지용 머신러닝 및 딥러닝 앙상블 모델 연구 김문석, 김형준, 김연우, 박진성(상명대학교)
	77	Transformer를 활용한 해시 기반 이미지 워터마킹 기법 최대호, 이영준, 손기욱, 이창훈(서울과학기술대학교)
	80	LLM-Mining: LLM을 활용한 크립토마이닝 공격의 가능성 평가 이한이, 최진우, 김진우(광운대학교)
	87	Windows Recall 아티팩트 분석 연구 김정아(성신여자대학교), 이산(단국대학교), 김도현(경북대학교), 김성윤(경일대학교), 이원희(부경대학교), 박경재(HM Company), 박상호(알파인랩)
	89	전력설비들의 사이버 위협 사례 분석과 공격 대응 전략에 대한 연구 박윤근(한국에너지공과대학교), 김량수, 유학(한국전자통신연구원), 이현우(한국에너지 공과대학교)
	91	IoT 기기 취약점 분석을 위한 LLM 기반 퍼징 기술 동향 이규원(동국대학교), 조효진(연세대학교)
	92	CSPM 솔루션을 활용한 AWS 클라우드 보안 규정 준수 자동화 김경필, 김규리, 이선경, 정대용, 정준호(동국대학교)
	165	Open-Source CSPM 기반의 클라우드 환경 컴플라이언스 준수 및 개인정보 보호 최적화 모델 제안 최승용(청주대학교), 장한나(성신여자대학교), 박현재(아주대학교), 전해준(충남대학교), 지한별, 권현준(KITRI Best of Best), 이해영(청주대학교)
	233	VDI(Virtual Desktop Infrastructure)와 다중보안체계(Multi-level Security)의 해외 사례 분석을 통한 보안성 강화 연구 안가은(서울여자대학교), 김다희(고려대학교), 이지수(가천대학교), 서다인(서울여자대학교), 이가현(조선대학교)
	95	블록체인 기반 공급망 보안 솔루션 설계 송현준(건국대학교), 김규진(부경대학교), 김민수(순천향대학교), 박수빈(전북대학교), 송태현(중부대학교)
	173	Apple 장치 보안 기술 우회 방안 분석 (발표분야: 디지털 포렌식, 학부생 논문) 진건승, 장진수(충남대학교)
	190	QR 코드 피싱 대응 방안에 대한 동향 이인석, 조대인, 홍득조(전북대학교)
	28	개발제한구역 내 건물변화탐지 인공지능의 성능 분석 연구 김영현(서울디지털재단)

◈ 주요 행사 및 프로그램 장소 안내

E빌리지 B1F



E빌리지 B2F



포스터세션

참가자 등록대 (그랜드 볼룸 앞)

	E빌리지 B1F – 컨퍼런스 L1~L5		E빌리지 B2F – Opus 2, 그랜드 볼룸	
	컨퍼런스 L1~L5		Opus 2	그랜드 볼룸
Day1	구두세션 포스터세션 기업소개 및 채용설명회 진행			신진연구자 소개 초청강연, 개회식, 정기총회 진행
Day2	구두세션 진행		–	

◈ 식사 제공 및 장소 안내

일자	내용	시간	장소
11/28 (목)	중식	12:00~13:00	카페테리아(스키하우스 2F)
	만찬	19:00~	학생: 그랜드 볼룸 앞(E빌리지 B2F), 일반: 미라시아(빌리지센터 1F)
11/29 (금)	조식	08:00~09:00	카페테리아(스키하우스 2F)
	중식	11:40~13:00	카페테리아(스키하우스 2F)

◈ 단체행사 지상 차량등록

- 학술대회 홈페이지 행사장 안내 하단에 링크에 들어가시어 주차 등록하시면 지상 주차 무료입니다.
- www.cisc.or.kr → 행사장 안내 탭 하단 차량 등록 링크 접속
- 예약번호: 23794597
- 고 객 명: 한국정보보호학회
- 행 사 명: 한국정보보학회
- 행사일자: 2024-11-28~2024-11-29
- 차량등록야외 주차장 위치 : 5, 6, 7번 주차장(차량 미 등록 시 이용불가)

Memo

Memo


오늘을 지키는 기술, 세상을 향한 혁신
GO FORWARD
FOR WORLD
Leading Innovation Group
LIG

2024년 한국정보보호학회 동계학술대회

CISC-W'24

Conference on Information Security and Cryptography Winter 2024

2024년 11월 28일(목)~29일(금) | 곤지암 리조트