2024년 한국정보보호학회 하계학술대회

CISC-S'24

Conference on Information Security and Cryptography Summer 2024

일자 2024년 6월 20일(목) ~ 21일(금)

장소 세종시 정부세종컨벤션센터

주최 한국정보보호학회 Korea Institute of Information Security & Cryptology

주관 고려대학교 세종캠퍼스 KOREA UNIVERSITY SEJONG CAMPUS

후원 국가정보원 NATIONAL INTELLIGENCE SERVICE · 과학기술정보통신부 · 행정안전부 · 세종특별자치시 · 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

한국정보보호학회
Korea Institute of Information Security & Cryptology

학술대회장

한국정보보호학회 회장 하재철

프로그램 위원회

- 프로그램위원장 이문규 (인하대학교) 윤종희 (영남대학교)
- 프로그램위원 권동현 (부산대학교) 권태경 (연세대학교)
  권현수 (인하대학교) 김도훈 (경기대학교)
  김종성 (국민대학교) 김태성 (충북대학교)
  김형식 (성균관대학교) 김형종 (서울여자대학교)
  김호원 (부산대학교) 김환국 (국민대학교)
  김휘강 (고려대학교) 노희준 (인하대학교)
  도경화 (고려대학교) 류권상 (공주대학교)
  박기웅 (세종대학교) 박정수 (강남대학교)
  서민혜 (덕성여자대학교) 서석충 (국민대학교)
  서승현 (한양대학교) 서화정 (한성대학교)
  양대헌 (이화여자대학교) 윤명근 (국민대학교)
  이경률 (목포대학교) 이석준 (가천대학교)
  이윤경 (한국전자통신연구원) 이종혁 (세종대학교)
  이창훈 (서울과학기술대학교) 이태진 (호서대학교)
  임을규 (한양대학교) 장대희 (경희대학교)
  최대선 (숭실대학교) 최선오 (전북대학교)
  최원석 (고려대학교) 최윤호 (부산대학교)

운영위원회

- 운영위원장 김희석 (고려대학교) 김창훈 (대구대학교)
- 운영위원 김원호 (국가보안기술연구소) 김정녀 (한국전자통신연구원)
  송중석 (한국과학기술정보연구원) 오진영 (한국인터넷진흥원)

우수논문상

구분	논문명	저자
과학기술정보통신부 최우수논문상	RoBERTa 기반 난독화된 실행 바이너리 코드 유사도 탐지	권유정, 엄지용, 구형준(성균관대학교)
행정안전부 최우수논문상	Grover 알고리즘 기반 ASCON 양자보안비도 분석을 위한 양자 회로 설계	오진섭, 최찬호, 최두호 (고려대학교)
세종시 세종시장 최우수논문상	HIGHT에 대한 결합 확률 분포 기반 분석	이인훈, 김규상,김준섭,박수진,김희석,홍석희 (고려대학교)
학회 최우수논문상	NTRU+KEM의 이항식 파라미터 제안	이미라, 이승우, 김종현(고려대학교), 박종환 (상명대학교)
한국인터넷진흥원 우수논문상1	DRAM 오류 주입 기반 인공 신경망 오분류 취약점 분석	김주환, 한동국 (국민대학교)
한국인터넷진흥원 우수논문상2	terSIDH의 아이소제니 연산 순서에 따른 성능 및 보안 분석	강태훈, 허동회, 이정환(고려대학교), 김수리(성신여자대학교), 홍석희 (고려대학교)
한국전자통신연구원 우수논문상1	고속도로 환경에서의 운전 행동 결정에 대한 적대적 공격 및 대응 시스템	이승열, 하재철 (호서대학교)
한국전자통신연구원 우수논문상2	KpqC 2라운드 AIMer에 대한 비밀키 복구 부채널분석 기법	한재승, 한동국 (국민대학교)
국가보안기술연구소 우수논문상1	얼굴 인증 시스템의 인증 가능한 강건성에 대하여	백승훈, 김동수, 황찬우, 김선필, 서재홍 (한양대학교)
국가보안기술연구소 우수논문상2	블록암호 MGFN의 전체 라운드에 대한 선형 공격	김남일, 임진한, 전용진, 백승준, 김종성 (국민대학교)
한국과학기술정보연구원 우수논문상 1	활성 상태 Windows 시스템에서의 DPAPI로 암호화된 자격증명 데이터 탐지 자동화 기법 연구	김재욱, 김준호, 박정흠(고려대학교)
한국과학기술정보연구원 우수논문상 2	fsync를 활용한 SSD 은닉채널 공격	고준석, 김태훈, 신영주(고려대학교)
학회 우수논문상	DNN의 은닉층에 대한 클럭 글리치 오류 주입 공격	강효주, 홍성우, 이영주, 하재철(호서대학교)
학회 우수논문상	Process hierarchy를 반영한 비정상 공격징후 탐지 기술 연구	윤주한, 정진욱, 이선우, 이태진(호서대학교)
학회 우수논문상	안전한 사물인터넷을 위한 이중 채널을 활용한 물리계층 보안	박채연, 이선진, 이일구 (성신여자대학교)
학회 우수논문상	악성 파일 탐지 모델 취약성 분석 및 방어 프레임워크	김명현, 조해현(숭실대학교)
학회 우수논문상	안드로이드 악성코드 패밀리 분류를 위한 시스템 콜 패턴 분석 연구	최재민, 최상훈, 박기웅(세종대학교)
학회 우수논문상	스마트팩토리 Blended Threat 자동 대응체계 개선을 위한 플레이북 오탐 패턴 분석 프로세스 연구	정인수, 송유래, 김득훈, 곽진 (아주대학교)
차세대 우수 여성과학자상 1	Kunerva+: 컨테이너를 위한 지능형 보안 정책 생성 프레임워크	김봄, 최유정, 이승수 (인천대학교)
차세대 우수 여성과학자상 2	경량 무선 펌웨어 업데이트를 위한 계층적 부분 퍼징 기법	김나현, 이진민, 이일구(성신여자대학교)
차세대 우수 여성과학자상 3	Blockchain-Edge-Cloud 통합을 이용한 안전한 유통망 모니터링 서비스	박예현, 신수진, 신상욱(부경대학교)

6월 20일(목)

시간	대연회장 (4F)	세션1 (중연회장(4F) -분할1)	세션2 (중연회장(4F) -분할2)	세션3 (소연회장1 (4F))	세션4 (소연회장2 (4F))	세션5 (소연회장3 (4F))	세션6 (VIP라운지 (4F))	세션7 (소회의실 (1F))
12:00~13:00	등록 (대연회장 앞 4F)							
13:00~14:30	포스터1	인공지능과 보안-1	IoT/ CPS보안-1		여성-1	소프트웨어 보안-1		암호이론과 구현-1
14:30~14:40	Break Time							
14:40~16:10	포스터2	인공지능과 보안-2	IoT/ CPS보안-2	여성-3	여성-2	소프트웨어 보안-2	네트워크 보안-1	암호이론과 구현-2
16:10~16:20	Break Time							
16:30~17:00	[초청강연] 국제회의장 4F 세종 지역산업현황 및 육성방안/윤석무 단장 (세종테크노파크)							
17:00~18:00	[개회식 및 시상] 국제회의장 4F 개회사 : 하재철 학회장 (한국정보보호학회) 환영사 : 김영 부총장 (고려대학교 세종) 축 사1 : 이승원 경제부시장 (세종시) 축 사2 : 황수훈 소장 (국가보안기술연구소) 행사보고 (최)우수논문 시상 경품추첨							

6월 21일(금)

시간	세션1 (중연회장(4F) -분할1)	세션2 (중연회장(4F) -분할2)	세션3 (소연회장1 (4F))	세션4 (소연회장2 (4F))	세션5 (소연회장3 (4F))	세션6 (VIP라운지 (4F))	세션7 (소회의실 (1F))
08:30-09:30	등록 (대연회장 앞 4F)						
09:00~10:30	인공지능과 보안-3	IoT/ CPS보안-3	시스템 보안-1	정보보호정책, 표준및인증	소프트웨어 보안-3	네트워크 보안-2	암호이론과 구현-3
10:30~10:50	Break Time						
10:50~12:20	인공지능과 보안-4	해킹과 취약점분석	시스템 보안-2	디지털포렌식	블록체인과 암호화폐	네트워크 보안-3	클라우드보안

구두발표 세션

2024. 6. 20(목)		
세션	논문번호	논문제목
13:00~14:30 세션1: 인공지능과 보안1	1	A Study of Domain Adaptation Techniques for Differentially Private Federated Learning 누룰 하지라 빈티 모하마드 놀, 최윤호 (부산대학교)
	30	IoT 트래픽에 대한 딥러닝 이상 탐지 성능 비교 이지원, 신재현 , 이정규, 윤주범 (세종대학교)
	31	파일 경로를 활용한 윈도우 이상 로그 탐지 기법 제안 조동규, 양인규, 정욱현 (세종대학교)
	34	Process hierarchy를 반영한 비정상 공격징후 탐지 기술 연구 정보보호학회 우수상 윤주한, 정진욱, 이선우, 이태진 (호서대학교)
	41	비전 트랜스포머를 위한 적대적 이미지 탐지 연구 박성규, 나현식(숭실대학교), 류권상(공주대학교), 최대선(숭실대학교)
	175	DNN의 은닉층에 대한 클럭 글리치 오류 주입 공격 정보보호학회 우수상 강효주, 홍성우, 이영주, 하재철 (호서대학교)
14:40~16:10 세션1: 인공지능과 보안2	46	인과추론 기반 객체 탐지 모델 취약점 분석 방안 이원호, 나현식(숭실대학교), 류권상(공주대학교), 최대선(숭실대학교)
	47	대규모 언어 모델에서 적대적 프롬프트의 위협: 재현 및 분석 박지훈, 최상훈, 박기웅(세종대학교)
	50	어텐션 메커니즘 기반의 이미지 분류 모델에 대한 적대적 공격 탐지 기법 심정현, 송현민 (단국대학교)
	51	고속도로 환경에서의 운전 행동 결정에 대한 적대적 공격 및 대응 시스템 ETRI 우수논문상 이승열, 하재철 (호서대학교)
	164	다크웹 범죄 프로파일링을 위한 자연어 처리 기반 사용자 행위 분류 기법 연구 장예진, 한지훈, 장성훈, 김호준, 김다슬, 한미란 (고려대학교)
	202	VANET에서 LSTM-VAE 모델을 활용한 Sybil 공격 탐지 이민종, 하재철 (호서대학교)
13:00~14:30 세션2: IoT/CPS보안1	45	HIGHT에 대한 결합 확률 분포 기반 분석 세종특별자치시장상 이인훈, 김규상, 김준섭, 박수진, 김희석, 홍석희 (고려대학교)
	61	전자기파 부채널 분석 기반 이상 행위 탐지 알고리즘 구현 및 개선 최민식, 박수진, 배대현(고려대학교), 정창민(국방과학연구소), 정영규(YM-나올텍), 김희석, 홍석희(고려대학교)
	180	프라이버시 침해가 제거된 원본 비디오 영상을 생성하는 프라이버시 카메라와 이의 활용 가능성 실험 김호영, 정경미, 최찬호, 이상만, 한미란, 최두호 (고려대학교)
	183	양자내성암호의 RISC-V 기반 하드웨어 가속기 연구 동향 최용렬, 김영범, 서석충 (국민대학교)
	193	곱셈 명령어가 제한된 환경에서 다항식 곱셈 연구 김영범, 서석충 (국민대학교)
	201	안전한 사물인터넷을 위한 이중 채널을 활용한 물리계층 보안 정보보호학회 우수상 박채연, 이선진, 이일구 (성신여자대학교)

2024. 6. 20(목)		
세션	논문번호	논문제목
14:40~16:10 세션2: IoT/CPS보안2	97	공개 펌웨어 수집 도구 설계 및 개발에 관한 연구 이인혁, 정수은, 박정흠 (고려대학교)
	101	원자력발전 테스트베드 데이터수집 및 분석 방법 김성아, 한준서, 아비섹 차우드하리, 최선오(전북대학교)
	107	드론 펌웨어의 보안을 위한 안티디버깅 기법 연구 연동현, 장대희 (경희대학교)
	110	사물인터넷(IoT)의 정책 동향과 국내 정책 강화를 위한 IoT BOM 제안 유현아, 이만희 (한남대학교)
	128	차량용 이더넷 환경에서의 SOME/IP 보안 연구 동향 박수연, 전희도, 최원석 (고려대학교)
	133	EMI 신호 주입을 활용한 UART 통신 간 Start Bit 탐지 기법 김의진, 조현수, 최원석 (고려대학교)
14:40~16:10 세션3: 여성3	98	동형 암호 기술 연구 동향 우나륜, 유지현 (광운대학교)
	115	차량용 진단 프로토콜의 보안 위협 및 대응 방안 연구 한태희, 변연희, 김서연, 김태근 (순천향대학교)
	167	EDR: 고효율 고신뢰 펌웨어 퍼징을 위한 이벤트 데이터 레코딩 기법 지승하, 한동임, 전소은, 이일구 (성신여자대학교)
	182	Proxy Re-encryption을 적용한 멀티 키 동형암호의 효율적인 복호화 알고리즘 서가영, 서민혜 (덕성여자대학교)
	200	경량 무선 펌웨어 업데이트를 위한 계층적 부분 퍼징 기법 차세대 우수여성과학자상 김나현, 이진민, 이일구 (성신여자대학교)
	213	채널 상태 정보 기반의 적응형 무선 펌웨어 업데이트 메커니즘 이승은, 이진민, 이일구 (성신여자대학교)
13:00~14:30 세션4: 여성1	7	블록체인 환경에서 DiSE 기법을 이용한 차량 사고기록데이터 거래 모델 신수진, 박예현, 신상욱 (부경대학교)
	29	클라우드 서버를 활용한 URL 미리보기 시스템 구축 서예린, 김유진, 박주희, 김성욱 (서울여자대학교)
	58	Kunerva+: 컨테이너를 위한 지능형 보안 정책 생성 프레임워크 차세대 우수여성과학자상 김봄, 최유정, 이승수 (인천대학교)
	69	위협 모델링을 통한 PLC 대상 UPS 분석 및 IEC 62443 보안 요구사항에 대한 위협 도출 최현서, 전규현, 진호준, 서정택 (가천대학교)
	71	격자 기반 서명에서 효율적인 기각 샘플링을 위한 상한 연산 방법 분석 곽현지(성신여자대학교), 우 주, 홍가희(고려대학교), 박종환(상명대학교), 이동훈(고려대학교)
	111	Modbus/TCP 기반 산업 시설의 취약점 탐지를 위한 공격 패킷 주입 시스템 개발 및 오류처리 메커니즘 연구 정수미, 문지윤, 김성환, 이지은, 송재승 (세종대학교)

2024. 6. 20(목)		
세션	논문번호	논문제목
14:40~16:10 세션4: 여성2	76	Blockchain-Edge-Cloud 통합을 이용한 안전한 유통망 모니터링 서비스 차세대 우수여성과학자상 박예현, 신수진, 신상욱 (부경대학교)
	91	NTRU+KEM의 이항식 파라미터 제안 정보보호학회 최우수상 이미라, 이승우, 김종현(고려대학교), 박종환(상명대학교)
	92	경량 블록암호 PIPO에 대한 두 바이트 오류 기반 차분 오류 공격 박혜진, 한재승, 한동국 (국민대학교)
	93	AES-CBC 모드에 대한 암호문 단독 상관전력분석 기법 노혜빈, 김주환, 한동국 (국민대학교)
	102	모방공격을 이용한 화이트 리스트 기반 시스템 호출 필터링 우회 기법 주송아, 장혜린, 신영주 (고려대학교)
	77	전자기파 스펙트럼 분석을 통한 멀티 코어 시스템의 효율적인 이상행위 탐지 방안 연구 박수진, 배대현, 최민식(고려대학교), 정창민(국방과학연구소), 정영규(YM-나올텍), 김희석, 홍석희(고려대학교)
13:00~14:30 세션5: 소프트웨어 보안1	11	Dynamic Analysis of Obfuscated Code with a 64-bit SGN Packer 엄지용, 전형준, 구형준 (성균관대학교)
	13	Lattigo 라이브러리를 이용한 동형암호 고성능 구현 방법 연구 최원빈(네이버클라우드), 김지훈(성균관대학교), 석상윤, 최현민(네이버클라우드)
	15	RoBERTa 기반 난독화된 실행 바이너리 코드 유사도 탐지 과기정통부 장관상 권유정, 엄지용, 구형준 (성균관대학교)
	137	제한된 범위의 정수 계수 다항식의 FFT 연산에 대한 SASCA 김규상, 이정환, 김희석, 홍석희 (고려대학교)
	163	소프트웨어 공급망 보안을 위한 AI(Artificial Intelligence)·ML(Machine Leraning) BOM 동향 분석 정윤정, 이준희, 이만희 (한남대학교)
	165	이진 분류 DNN 모델에서 클럭 글리치를 이용한 오분류 공격과 대응방안 홍성우, 강효주, 이영주, 하재철 (호서대학교)
14:40~16:10 세션5: 소프트웨어 보안2	196	양자내성암호 전환을 위한 퍼징을 활용한 암호 알고리즘 구현 취약점 분석 동향 신동현, 서석충 (국민대학교)
	99	KpqC 2라운드 후보 SMAUG-T의 키종속 연산에 대한 단순전력분석 및 대응기법 유성환, 한재승, 한동국(국민대학교)
	104	FPGA AES 설계 중간값에 따른 딥러닝 기반 프로파일링 분석 성능 비교 오충연, 최기훈, 김주환, 한동국(국민대학교)
	186	Cortex-M4에서의 Falcon 구현 최적화 연구 최준혁, 서석충 (국민대학교)
	204	스마트팩토리 Blended Threat 자동 대응체계 개선을 위한 플레이북 오탐 패턴 분석 프로세스 연구 정보보호학회 우수상 정인수, 송유래, 김득훈, 곽진 (아주대학교)
	207	terSIDH의 아이소제니 연산 순서에 따른 성능 및 보안 분석 KISA 우수논문상 강태훈, 허동회, 이정환(고려대학교), 김수리(성신여자대학교), 홍석희(고려대학교)

2024. 6. 20(목)		
세션	논문번호	논문제목
14:40~16:10 세션6: 네트워크 보안1	12	동형암호를 활용한 프라이버시 보존 피싱 URL 탐지 기법 석상윤, 최현민 (네이버클라우드)
	113	프로그래머블 스위치를 이용한 패킷 간 지연 시간 이용 VoIP 워터마크 탐지 유한 상태 기계 백승진, 김동혁, 강민석 (KAIST)
	148	RSA-CRT에 대한 수동적 오류 주입 공격 동향 이상원, 김수형, 인범식, 이영주, 하재철 (호서대학교)
	153	TLS 1.3 0-RTT 모드의 효율성 분석을 위한 성능 실험 연구 김영재, 원태호, 김보남, 유일선 (국민대학교)
	179	암호화된 트래픽 분류 성능 향상을 위한 준지도학습 기반 데이터 라벨링 기법 연구 최대호, 조민정, 손기욱 (서울과학기술대학교)
	191	오토인코더 기반 암호트래픽 분석기술 동향 김찬형, 윤종희 (영남대학교)
13:00~14:30 세션7: 암호이론과 구현1	94	KpqC 2라운드 AIMer에 대한 비밀키 복구 부채널분석 기법 ETRI 우수논문상 한재승, 한동국 (국민대학교)
	112	국산 블록암호 알고리즘을 이용한 PACS 데이터 인증 암호화 전승혁, 김아은(전북대학교), 김용식(고려대학교), 홍득조 (전북대학교)
	116	SSH 상에서 하이브리드 양자내성 키 교환 알고리즘 평가 오훈, 박문기, 이세영 (강원대학교)
	118	32-bit RISC-V 아키텍처에서 ARX 기반 경량 블록암호 SPECK32와 CHAM64의 최적 병렬 구현 신명수, 신한범(고려대학교), 홍득조(전북대학교), 성재철(서울시립대학교), 홍석희(고려대학교)
	122	블록암호 SIMON에 대한 양자 회로 최적화 구현 김남일, 백승준, 전용진, 김기윤, 김종성 (국민대학교)
	130	PQC 전자서명 추가공모전 라운드 1의 MPC-in-the-Head 전자서명 분석 장지훈, 이정환, 이명훈(고려대학교), 김수리(성신여자대학교), 홍석희(고려대학교)
14:40~16:10 세션7: 암호이론과 구현2	131	블록암호 MGFN의 전체 라운드에 대한 선형 공격 NSR 우수논문상 김남일, 임진한, 전용진, 백승준, 김종성(국민대학교)
	144	96-비트 비밀키를 갖는 12-라운드 DABC 블록암호에 대한 선형공격 송원우, 강성민, 전용진, 김종성 (국민대학교)
	177	저사양 16-bit MSP430 환경에서의 NTT 기반 Saber 최적화 연구 김민기, 신동현, 김영범, 서석충(국민대학교)
	188	AES-GCM 운용모드에 대한 구현 방법론 동향 분석 이재석, 김동천, 서석충 (국민대학교)
	189	암호 분야에서의 정형 검증 연구 동향 분석 지용현, 김영범, 서석충 (국민대학교)
	194	V2X 인증서 관리 표준 SCMS에 대한 양자내성암호 적용 연구 한윤선(국민대학교), 김동민(삼성전자), 서석충 (국민대학교)

구두발표 세션

2024. 6. 21(금)		
세션	논문번호	논문제목
09:00~10:30 세션1: 인공지능과 보안3	27	머신러닝을 이용한 IoT 트래픽 이상 탐지 성능 분석 신재현, 이지원, 유지현, 윤주범(세종대학교)
	59	얼굴 인증 시스템의 인증 가능한 강건성에 대하여 NSR 우수논문상 백승훈, 김동수, 황찬우, 김선필, 서재홍 (한양대학교)
	74	워드 임베딩 기반의 Windows 파일 경로 이상 탐지 이라경, 송현민 (단국대학교)
	80	인공지능을 활용한 의심 윈도우 로그 추천 시스템 최성훈, 진현준, 김주성, 민성주, 신정훈, 윤주범 (세종대학교)
	103	Gaussian Noise-adding 기법을 통한 딥보이스 탐지 성능 개선 및 적대적 공격 방어 김인호, 류태원, 홍기훈, 정수환(숭실대학교)
	178	멤버십 추론 공격을 방어하기 위한 GAN 기반 데이터 합성 기법 정예림, 김소연, 이일구 (성신여자대학교)
10:50~12:20 세션1: 인공지능과 보안4	109	한국어 대규모 언어모델에 대한 개인정보 데이터 추출 공격 연구 장현준, 박대얼, 최대선 (숭실대학교)
	121	악성 파일 탐지 모델 취약성 분석 및 방어 프레임워크 정보보호학회 우수상 김명현, 조해현 (숭실대학교)
	125	LFCC와 LSTM을 활용한 딥페이크 오디오 탐지 기법 박성빈, 송현민 (단국대학교)
	126	퍼징 성능 향상을 위한 대규모 언어 모델의 활용: 취약점의 근본 원인과 관련 필드 분석을 통한 초기 입력값 생성에 대하여 박상현, 이하은, 차상길 (KAIST)
	147	마스킹된 인공 신경망을 위한 2-Sharing 정수 비교 연산 김준섭. 김규상, 박수진, 김희석, 홍석희 (고려대학교)
	185	딥러닝 가속기에 대한 오류주입공격 및 대응기술 연구 동향 강은세, 윤동욱, 김호원 (부산대학교)
09:00~10:30 세션2: IoT/CPS보안3	135	LoRa 기반 IoT 시스템 보안 취약점 및 대응 방안 김성훈, 전희도, 최원석 (고려대학교)
	152	딥러닝 기반 시계열 이상 탐지 연구 동향 윤지원, 김호원 (부산대학교)
	157	멀티 코어 프로세서의 전자기파 부채널 누출 특성 분석 배대현,박수진, 최민식(고려대학교),정창민(국방과학연구소),정영규(YM-나을텍),김희석,홍석희 (고려대학교)
	159	HITL 시뮬레이션과 실제 환경에서의 HackRF를 이용한 드론 공격 시나리오 오진섭,이한빈, 조리노, 조준영, 이상만, 최두호, 한미란 (고려대학교)
	160	RF 신호 분석을 통한 합성곱 신경망(CNN) 기반 드론 식별 연구 오진섭, 이한빈,조리노,조준영, 이상만, 최두호, 한미란 (고려대학교)
	171	IoT 기기 보안 점검을 위한 쉘 확보 방법론 연구 윤민규, 이경수, 홍승표 (코어시큐리티)

2024. 6. 21(금)		
세션	논문번호	논문제목
10:50~12:20 세션2: 해킹과 취약점분석	8	기호 실행을 이용한 바이너리 기반 Double Free 취약점 탐지 기법 김동주, 김동수, 신영주 (고려대학교)
	26	NLP기반 익스플로잇 코드 생성 자동화 시스템 설계 진규정(강원대학교), 임정우(한신대학교), 장한나(성신여자대학교), 이효찬, 배송현(고려대학교), 최민석(대구가톨릭대학교), 최준원(경희사이버대학교)
	35	공격자 관점에서 SBOM 기반 소프트웨어 공급망의 공격 표면 분석 프레임워크 조윤정, 박후린 (서울여자대학교)
	68	최신 오픈소스 취약점 사례와 대응 방법 신성욱, 이세영 (강원대학교)
	89	DRAM 오류 주입 기반 인공 신경망 오분류 취약점 분석 KISA 우수논문상 김주환, 한동국 (국민대학교)
	140	의료기관 대상 의료데이터 해킹 사례 분석 및 대응 정소이, 김우진, 박상원, 이세영 (강원대학교)
09:00~10:30 세션3: 시스템 보안1	2	fsync를 활용한 SSD 은닉채널 공격 KISTI 우수논문상 고준석, 김태훈, 신영주 (고려대학교)
	6	Open Quantum Safe 프로젝트 동향 및 벤치마크 김현준, 서화정 (한성대학교)
	24	펄스 폭 변조를 이용한 ECU 차동 전압 변화 실험 환경 박경록(단국대학교), 이정호(씨피식스), 우사무엘(단국대학교)
	42	Pseudo-BERT-C : 의사 레이블 기반 사이버 공격클래스 다중 분류 기술 이준영, 김태현, 김태은, 임준형 (한국인터넷진흥원)
	129	보이스피싱 수사를 위한 워터마크 삽입 기술 및 VoIP 프로토콜 분석 김덕우, 안준호, 오범석, 김광민, 오택경, 박철준, 김용대 (KAIST)
	132	Kadapter: Kata Container를 위한 런타임 보안 집행 프레임워크 조치현, 허진, 이승수 (인천대학교)
10:50~12:20 세션3: 시스템 보안2	19	RDA를 활용한 Windows 드라이버 DeviceIoControl 처리함수 탐지 박찬희, 송가현, 신영주 (고려대학교)
	44	변형 샘플을 통한 VirusTotal 탐지 특성 연구 반영훈, 오세환, 조해현 (숭실대학교)
	62	이기종 보안장비 이벤트 분석을 위한 AI 기반의 정규표현식 자동 생성 방안 연구 김태현, 이새움, 김태은, 이준영, 임준형 (한국인터넷진흥원)
	119	LLM을 이용한 코드 난독화 기법 분류 강준혁, 이지원, 진홍주, 최원석, 이동훈 (고려대학교)
	138	오픈 랜(Open-RAN) 환경의 보안 위협 및 대응 방안에 대한 글로벌 동향 김홍년, 윤요섭, 오인수, 임강빈 (순천향대학교)
	139	실시간 CAN 공격-방어 시나리오 구현을 위한 임베디드 시스템 기반 트랜시버 개발 류동현, 정민찬, 유근영, Md Rezanur Islam, Munkhdelgerekh Batzorig, 임강빈 (순천향대학교)

2024. 6. 21(금)		
세션	논문번호	논문제목
09:00~10:30 세션4: 정보보호정책, 표준 및 인증	10	Lite TARA: Lite Threat Analysis and Risk Assessment 장민영, 오준희, 우사무엘 (단국대학교)
	108	국내외 개인정보 침해 관련 다크패턴 유형 비교 분석 김홍길, 이세영 (강원대학교)
	120	UNR 사이버 보안 규제 요구 사항에 따른 개별 ECU 기반의 TARA 테스트 자동화 정민찬, 황지웅, 김홍년, 김윤지, 오인수, 임강빈 (순천향대학교)
	150	랜덤오라클 없는 양자내성 패스워드기반 키공유 프로토콜 연구 김현서, 이예솔, 황정연 (성신여자대학교)
	141	CycloneDX 1.6 업데이트 내용 소개 김지민, 손현승, 이만희 (한남대학교)
	190	공급망 보안을 위한 SBOM 도입 및 활성화 방안 김세린, 김수연 (성신여자대학교)
10:50~12:20 세션4: 디지털포렌식	25	안드로이드 환경에서의 네이버 밴드 로컬 아티팩트 분석 안원석, 박명서 (한성대학교)
	28	Linux 환경을 대상으로 한 RansomEXX 및 Monti 랜섬웨어 동작 분석 김한결(강남대학교), 위다빈, 박명서 (한성대학교)
	39	협업 툴 Kakao Work 데이터베이스 포렌식 분석 김강한(국민대학교), 김현준(세종대학교), 박진철, 박지수, 강수진, 김종성 (국민대학교)
	73	Graph Neural Network를 활용한 분석 방지 보호 기법 탐지 방안 연구 임소미, 유현준, 최서연, 유지현 (광운대학교)
	134	MAVLink를 이용한 커스텀 드론 데이터 추출 기법 연구 이철한, 성민규, 윤우성, 박정흠 (고려대학교)
	142	안드로이드 환경에서의 SecNeo 패커 기반 애플리케이션 안티 디버깅 기법 분석 연구 전유민, 정수은(고려대학교), 김도현(부산가톨릭대학교), 이상진, 박정흠 (고려대학교)
09:00~10:30 세션5: 소프트웨어 보안3	88	카운터메저에 대한 효율적 적대적 학습 방법 우승민, 홍기훈, 정수환 (숭실대학교)
	95	ODROID XU4 Exynos5422(Cortex-A15/A7) 환경에서 KYBER와 SMAUG-T의 성능 비교 및 분석 박지민, 윤성우, 목정현, 이석준 (가천대학교)
	123	산업 기반 시설 테스팅을 위한 시나리오 기반 공격 패킷 생성 기술 연구 문지윤, 정수미, 김성환, 이지은, 송재승 (세종대학교)
	136	활성 상태 Windows 시스템에서의 DPAPI로 암호화된 자격증명 데이터 탐지 자동화 기법 연구 KISTI 우수논문상 김재욱, 김준호, 박정흠 (고려대학교)
	187	Cortex-M4 마이크로컨트롤러에서 HQC 알고리즘 최적화 전략 이명훈, 장지훈(고려대학교), 김수리(성신여자대학교), 홍석희 (고려대학교)

2024. 6. 21(금)		
세션	논문번호	논문제목
10:50~12:20 세션5: 블록체인과 암호화폐	117	공개키 기반 임계 암호 기법 동향 조사 백진현, 김준식(고려대학교), 박종환 (상명대학교)
	151	대규모 실시간 IIoT 데이터 처리를 위한 블록체인 활용 무결성 검증 시스템 성능 분석 문예찬, 권호석, 김보남, 유일선 (국민대학교)
	158	난독화된 AES에 대한 차분 계산 분석 염지훈, 정상윤, 신원근, 김희석 (고려대학교)
	192	LLM을 활용한 스마트 컨트랙트 취약점 탐지 연구 동향 분석 김재현, 이상명, 김호원 (부산대학교)
	208	큰 수에 대한 모듈러 연산에 효율적인 Barrett Reduction 양자 회로 구현 이창열, 장건, 조성민, 서승현 (한양대학교)
	214	양자 NTT 회로 최적화 구현 조성민, 이창열, 장건, 서승현 (한양대학교)
09:00~10:30 세션6: 네트워크 보안2	198	NCC-Sign(Non-Cyclotomic)에서의 효율적인 다항식 곱셈을 위한 NTT 적용 방안 연구 고우형, 김영범, 서석충 (국민대학교)
	205	암호화된 군 네트워크 트래픽 분석을 위한 feature 추출 프로세스 연구 정인수, 김득훈(아주대학교), 임선영 (LIG넥스원), 곽진(아주대학교)
	33	Network topology를 반영한 IP레벨에서의 공격행위 탐지 기술 연구 이주영, 이선우, 황상연, 이태진 (호서대학교)
	36	안드로이드 악성코드 패밀리 분류를 위한 시스템 콜 패턴 분석 연구 정보보호학회 우수상 최재민, 최상훈, 박기웅 (세종대학교)
	81	OCR 기반 안드로이드 비싱 애플리케이션 탐지 기법 김대겸, 조해현 (숭실대학교)
	105	개인정보보호를 고려한 P2P 전력거래를 위한 분산 ESS환경의 통합관리 웹 시스템 및 사용자 인터페이스 설계 김소은, 홍유진, 김나연, 김민주, 김정현, 김형종(서울여자대학교)
10:50~12:20 세션6: 네트워크 보안3	143	SQIsign2D-West에 대한 오류 주입 공격 이정환, 허동회, 김규상, 김희석, 홍석희 (고려대학교)
	96	축소 마스킹 대응기법에 대한 딥러닝 기반 부채널공격 취약점 분석 오성빈, 김주환, 한동국 (국민대학교)
	106	스마트 그리드 대상 사이버 복원력 연구 동향 분석 박미리, 고아름, 이주현, 서정택 (가천대학교)
	114	스마트폰 무음 소리 재생을 이용한 전자파 신호 은닉 채널 형성 방안 김용재, 안현준, 한동국 (국민대학교)
	149	안드로이드 환경에서의 랜덤채팅 어플리케이션 엠티와 썸톡 아티팩트 분석 위다빈(한성대학교), 김한결(강남대학교), 박명서(국민대학교)
	155	Kou et al.이 제안한 UAV 대상 ECDH 기반 키 합의 프로토콜의 정형화 검증 오지언, 우창현, 박영신, 고용호, 유일선 (국민대학교)

2024. 6. 21(금)		
세션	논문번호	논문제목
09:00~10:30 세션7: 암호이론과 구현3	100	KpqC 2라운드 전자서명 HAETAE에 대한 상관전력분석 조홍래, 한재승, 한동국 (국민대학교)
	197	Cortex-M4 상에서의 HQC 구현 및 성능 분석 김동천, 서석충 (국민대학교)
	199	초특이 아이소제니 기반 해시 함수 연구 허동회, 이정환, 강태훈(고려대학교), 김수리(성신여자대학교), 홍석희(고려대학교)
	209	ECB 모드 암호의 일방향성 안전성과 구별 불가능성 안전성에 관한 연구 김동현, 박동현, 김민지, 이제원, 김동찬 (국민대학교)
	210	Controlled ADDER 최적화 양자 회로 구현 전찬호, 홍석희 (고려대학교)
	212	Grover 알고리즘 기반 ASCON 양자보안비도 분석을 위한 양자 회로 설계 **행정안전부 장관상** 오진섭, 최찬호, 최두호 (고려대학교)
10:50~12:20 세션7: 클라우드 보안	14	Terraform을 이용한 클라우드 인프라 에디터 개발 및 개인정보 보호를 위한 IaC 코드 안전성 연구 이호정, 이지은, 김수린, 한채림, 김형종 (서울여자대학교)
	63	SaaS 보안 위협과 MITRE ATT&CK 기반 자동화 매핑 방안 제고 김수현, 최정원, 이송하, 박후린 (서울여자대학교)
	127	CATS : 마이크로서비스 프로세스 안티-템퍼링을 통한 공격 탐지 방안 연구 김상현, 최상훈, 박기웅 (세종대학교)
	203	클라우드 환경에서의 국가핵심기술 보호조치 연구 : 접근통제 중심으로 정민서, 박승희, 이현정, 한명진 (성신여자대학교)
	162	한국어 특성을 고려한 한국 도메인 패스워드 취약점 분석 채민아, 신원근, 정상윤, 김희석 (고려대학교)
	173	생성형 AI 기반 워터마크 기술의 강인성 평가 김수경, 전유란, 류정화, 이일구 (성신여자대학교)

2024. 6. 20(목)		
세션	논문번호	논문제목
13:00~14:30 포스터1 6. 20(목)	3	NIST PQC 암호 최적화 구현 동향 엄시우, 송민호, 김상원, 서화정 (한성대학교)
	4	IoT 펌웨어에 대한 정적 오염 분석 연구 동향 이지혜, 박찬희, 신영주 (고려대학교)
	5	Rust 기반 암호 구현 기술 동향 김상원, 엄시우, 송민호, 서화정 (한성대학교)
	9	KpqC 암호 최적화 구현 동향 송민호, 엄시우, 김상원, 서화정 (한성대학교)
	16	CAN에 적용된 최신 MTD 기술 동향 유수연, 이정호, 우사무엘 (단국대학교)
	17	주요 보안 학회 통계를 통한 정보보호 동향 분석 백승혜, 오예진, 표자연, 신지선 (세종대학교)
	18	자율주행자동차와 V2X 통신의 보안 취약점 양혜연, 전서연, 신지선 (세종대학교)
	20	암호화된 GML 기반 OSS 검사 효율성에 대한 연구 장석준, 이임영, 김수현 (순천향대학교)
	21	블룸 필터 기반의 데이터 교차점 계산을 수행하는 DH-PSI에 관한 연구 김기환, 김수현, 이임영 (순천향대학교)
	22	IoT기술을 활용한 기숙사 세탁기 예약 애플리케이션 박주혁, 이덕규 (서원대학교)
	23	공용 세탁기 관리 및 예약 시스템 개발 박규범, 이덕규 (서원대학교)
	32	Attention Mechanism 기반으로 한 Honey Chatting 구현 가능성 전건우, 윤지원 (고려대학교)
	37	인스턴트 메신저 Bridgefy 데이터 복호화 및 아티팩트 분석 연구 안현종, 조동후, 박세준, 강수진, 김종성 (국민대학교)
	38	스마트 컨트랙트를 이용한 검색 가능한 암호화 김예은, 오희국 (한양대학교)
	40	DJI RC 동적 분석 환경 구축: 문제점과 해결책 홍표길, 이우진, 김종인, 김도현 (부산가톨릭대학교)
	43	Ubuntu 24.04 LTS의 보안 및 성능을 강화하는 고급기능 김혜정, 서예린, 송민희, 신지선 (세종대학교)
	48	Illusion-Injection: 고도화 된 악성코드 저지를 위한 디버깅 기술 연구 이재욱, 최상훈, 박기웅 (세종대학교)
	49	군 환경 내 네트워크 트래픽 이상 탐지 연구 동향 송유래, 김득훈(아주대학교), 임선영(LIG넥스원), 곽진 (아주대학교)

2024. 6. 20(목)		
세션	논문번호	논문제목
13:00~14:30 포스터1 6. 20(목)	52	대학 캠퍼스 실내 네비게이션 모델 연구 및 개발 박유안, 이덕규 (서원대학교)
	53	안전한 스마트 홈 환경을 위한 익명 인증에 대한 연구 윤성철, 김수현, 이임영 (순천향대학교)
	54	ZTA 환경에서 워크로드 간 재인증 효율성 향상 방안에 관한 연구 최원휘, 박정수 (강남대학교)
	55	ROS2의 보안 기능과 네트워크 성능 관계 연구 분석 홍가희, 최원석 (고려대학교)
	56	블록체인에서의 의료 데이터 프라이빗 연산: 동형 암호화, 영지식 증명, 다자간 계산을 이용한 fhEVM 유준수, 윤지원 (고려대학교)
	57	블루투스 비콘 기반 대학교 강의실 길 안내 시스템 : 서버의 중심 역할 김민기, 이덕규 (서원대학교)
	60	프로세스 인젝션을 통한 프로세스 보호 기법 연구 김지완, 장대희 (경희대학교)
	64	AWS 클라우드 환경에서 영향도에 따른 이벤트 로그 분류 방법 제안 이상운, 신재현, 이민욱, 정우성 (세종대학교)
	65	군집 드론에서 무인 항공 시스템 구성요소 간 인증 기술 동향 김세훈, 이하늘, 이종혁 (세종대학교)
	66	드론 간 통신에서의 보안 위협 및 요구사항 분석 이동욱, 이하늘, 이종혁 (세종대학교)
	85	oneM2M 기반 IoT 시스템을 위한 리소스 모델링 툴 개발 권수빈, 김주성, 신정훈, 진현준, 송재승 (세종대학교)

2024. 6. 20(목)		
세션	논문번호	논문제목
14:40~16:10 포스터2 6. 20(목)	67	점진적 가지치기를 통한 비대화형 암호화된 의사결정 트리 기반 질병 진단 홍미연, 윤지원 (고려대학교)
	70	NIST 표준 양자내성 서명 FALCON과 개량 알고리즘들의 비교 분석 김광조(국제사이버보안연구원/KAIST), 김연준 (엘지유플러스)
	72	데이터 특성에 따른 차분 프라이버시 적용 방안 연구 강태웅, 유지현 (광운대학교)
	75	OpenPLC의 Modbus 모듈에 대한 정적분석 조종진, 강미영 (고려대학교)
	78	AI 기반 악성코드 탐지 및 분류를 위한 악성코드 내 데이터 추출 방식 분석 정재원, 지일환, 이주현, 서정택 (가천대학교)
	79	국내외 RMF 도입에 관한 동향 분석 이호영, 손경호, 이세영 (강원대학교)
	82	AWS 서비스를 이용한 클라우드 보안 관제 시스템 조경수, 오준희, 문지윤 (세종대학교)
	83	기계학습 기반의 보안 직무분류체계 설계 최다인, 민무홍 (성균관대학교)
	84	온라인 불법 도박 검증 플랫폼 활용 모니터링 시스템 설계 신지호, 민무홍 (성균관대학교)
	86	PLC 제어로직 feature 별 relationship을 반영한 임베딩기반 이상탐지 방법 제안 이주현, 전승호, 서정택 (가천대학교)
	87	연합학습 기반 IoT 다중 SDN 컨트롤러 대상 이상 탐지 시스템 제안 이진규, 이주현, 서정택 (가천대학교)
	90	Face-Swapping 기법 기반 변조 모델에 따른 딥페이크 탐지 모델 성능 비교 분석 김아름, 최희원, 이주현, 서정택 (가천대학교)
	146	신뢰할 수 있는 환경 기반 딥러닝 연구 동향 분석 임유빈, 조해현 (숭실대학교)
	154	랜섬웨어 탐지 방법 연구 동향 분석 황연정, 조재한, 신다윗, 김호원 (부산대학교)
	156	프로세스 내 메모리 격리 기술 연구 동향 박성환, 송수현, 권동현 (부산대학교)
	161	형식 보존 암호화를 이용한 얼굴 비식별화 김희환, 박성준, 최대선 (숭실대학교)
	166	Leveraging Blockchain Technology for Enhanced Privacy in ESG Reporting: A Case Study in the Cosmetics Industry with a Focus on Reducing Marijuana Usage Cho Nwe Zin Latt, Igugu Tshisekedi Etienne, Kyung-Hyung Rhee (Pukyong National University)
	168	딥페이크 탐지 성능 검증을 위한 이미지 품질 평가 방법 분석 이재희, 김현준, 박래현, 권태경 (연세대학교)

2024. 6. 20(목)		
세션	논문번호	논문제목
14:40~16:10 포스터2 6. 20(목)	169	블록체인 기술을 사용한 메타버스 로그인 방식 분석 조원영, 김윤식, 황은비, 한상수, 권태경 (연세대학교)
	170	IEC 62443 기반 Threat Modeling을 통한 PLC 보안 강화 연구 윤민규, 임은서, 조이수 (코어시큐리티)
	172	스마트공장 환경에서의 도메인 온톨로지 기반 잠재 복합위협 식별 및 시각화 송유래, 김득훈, 곽진 (아주대학교)
	174	OT 공급망 보안 요구사항을 위한 IEC 62443 분석 이준희, 정윤정, 이만희 (한남대학교)
	176	화상회의 보안성 평가 지침에 관한 연구 김민지, 박동현, 이제원, 김동찬 (국민대학교)
	181	Soulbound Token을 활용한 자동 보험 청구 시스템 제안 정은혜, Cho Nwe Zin Latt, 이경현 (부경대학교)
	184	양자머신러닝에 활용되는 QAOA 알고리즘 예제 분석 최순욱, 최두호 (고려대학교)
	195	Research on Utilizing Similarity Learning for Log Anomaly Detection Based Pretrained Language Models 레리사 아데바 질차, 김득훈, 곽진 (아주대학교)
	211	양자 컴퓨팅 신뢰성 향상을 위한 양자 상태 제어 및 측정 기술 동향 이고은, 홍다희, 조성민, 서승현(한양대학교)
	215	오토인코더 기반 LSTM을 활용한 효율적인 이상 탐지 기법 이규원(동국대학교), 임서영(강남대학교), 이선진(성신여자대학교), 이일구 (성신여자대학교)

[등록비]

구분	회원	비회원	현장등록
일반	200,000	300,000	300,000
군·공무원	100,000	150,000	150,000
학생 (전일제)	100,000	150,000	150,000
학부생	50,000	50,000	50,000
시니어(63세 이상) 종신회원	무료		

- 군.공무원 등록은 주무관청에 소속 중인 공무원증 소지자에 한합니다. (국공립 교직원 제외)
- 시니어 무료등록은 학회 종신회원으로 1962년 12월 31일 이전 출생자에 한합니다.
- 학부생의 경우 kiisc@kiisc.or.kr 로 학생증 사본 송부해 주시기 바랍니다.
- 학회 특별회원사 임직원은 학회 회원으로 준합니다.
  특별회원사 여부는 학회 홈페이지 (www.kiisc.or.kr) 회원광장 → 특별회원사에서 확인하실 수 있습니다.
  (예시: 한국인터넷진흥원, 한국전자통신연구원, 국가보안기술연구소 등)
- 학생은 전일제에 한합니다. (타소속 없음)

[사전등록]

- 학회 홈페이지(www.kiisc.or.kr)에서 접속할 경우, 학회행사 → 사전등록바로가기 → 학술행사 선택(2024 하계학술대회) 등록하기 선택
- 사전등록 마감일:
  -논문 발표자: ~ 2024년 6월 9일(일)
  -일반 참가자: ~ 2024년 6월 17일(월)
- 계좌번호: 국민은행 754-01-0008-146 (예금주 한국정보보호학회)
- 무통장 입금 결제 시 등록비는 위의 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 영수증 계산서가 필요하신 경우 미리 학회로 연락바랍니다.
- 입금명은 소속명으로만 기재하여 입금 시 확인이 되지 않습니다.
  이에 등록 누락을 방지하고자 입금명은 필히 [행사명 첫글자+등록자 성함]으로 기재해 주시기 바랍니다.
  예) 하계학술대회 등록 홍길동-〉 "하홍길동" 기재
- 행사 종료 후 등록자의 핸드폰 번호로 모바일 상품권(학술대회 기념품)을 발송 드립니다.
  등록 시 핸드폰번호 미기재/오기입 시 재발송이 불가합니다.
- 등록확인서 및 참가확인서는 등록비 납부완료자에 한하여 한국정보보호학회 홈페이지 상단 "행사등록 및 참가확인서" 바로 가기를 클릭하신 후 등록 시 기재하신 성함과 이메일을 기재하시면 출력 가능합니다. (단, 참가확인서는 행사종료 후 다음날부터 발급 가능)
- 참석자 제공 사항: 프로그램북, 온라인 프로시딩(논문집), 모바일 행사 기념품

[문의처]

- 행사 문의처: 한국정보보호학회 사무국 02-564-9333(내선2), kiisc@kiisc.or.kr
- 계산서 문의처:한국정보보호학회 사무국 02-564-9333(내선3), kiisc@kiisc.or.kr

MEMO

2024년 한국정보보호학회 하계학술대회

CISC-S'24

Conference on Information Security and Cryptography Summer 2024