한국정보보호학회
Korea Institute of Information Security & Cryptology

2021년 한국정보보호학회 하계학술대회

CISC-S'21

Conference on Information Security and Cryptography Summer 2021

2021년 6월 24일(목)

온라인 컨퍼런스

(개회식 촬영: 한국과학기술회관 12F 아나이스홀)

주최 한국정보보호학회 Korea Institute of Information Security & Cryptology

주관 KAIST 한국과학기술원

후원 과학기술정보통신부 국가정보원 National Intelligence Service Korea 행정안전부

NSR 국가보안기술연구소 National Security Research Institute KISA 한국인터넷진흥원 ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute

쌍용정보통신주식회사 SsangYong Information & Communications Corp.

위원회

학술대회장 류재철 한국정보보호학회 회장

프로그램 위원회

- 프로그램위원장 이정현, 조해현 (숭실대학교)
- 프로그램위원

곽 진 (아주대학교)	구형준 (성균관대학교)
권태경 (연세대학교)	김범수 (연세대학교)
김성민 (성신여자대학교)	김소정 (국가보안기술연구소)
김영근 (숭실대학교)	김영식 (조선대학교)
김형종 (서울여자대학교)	김휘강 (고려대학교)
박기웅 (세종대학교)	백유진 (우석대학교)
변진욱 (평택대학교)	서정택 (가천대학교)
서화정 (한성대학교)	손태식 (아주대학교)
송도경 (연세대학교)	유일선 (순천향대학교)
윤주범 (세종대학교)	이광수 (세종대학교)
이덕규 (서원대학교)	이만희 (한남대학교)
이창훈 (서울과학기술대학교)	이태진 (호서대학교)
장대희 (성신여자대학교)	장항배 (중앙대학교)
전유석 (UNIST)	조효진 (숭실대학교)
최대선 (숭실대학교)	최원석 (한성대학교)
한동국 (국민대학교)	허준범 (고려대학교)
홍득조 (전북대학교)	

운영위원회

- 운영위원장 김용대 (KAIST)
- 운영위원

강민석 (KAIST)	윤인수 (KAIST)
장대희 (성신여자대학교)	장진수 (충남대학교)

우수논문상

구분	상장명	논문명	비고
최우수	과학기술정보통신부 장관상	안드로이드 어플리케이션의 개인정보 유출을 방지하기위한 민감한 데이터 흐름 보호 기법 전거창, 조해현, 이정현 (숭실대학교)	
최우수	행정안전부 장관상	스테레오 매칭 딥러닝 모델에 대한 최적화 기반 적대적 공격 심상훈 (고려대학교), 주경호 (고려대학교), 최원석 (한성대학교), 이동훈 (고려대학교)	
최우수	학회 최우수논문상 1	적대적 신경망 기반의 암호 설계 기술 연구 정수용, 홍도원, 서창호 (공주대학교)	
최우수	학회 최우수논문상 2	CAN 기반 전기차 충전 프로토콜 분석 강동우 (숭실대학교), 김다영 (서울여자대학교), 신지우 (서울여자대학교), 김형훈 (숭실대학교), 주경호 (고려대학교), 조효진 (숭실대학교)	
우수	국가보안기술연구소 소장상 1	블록암호의 양자회로 설계 연구 정건상 (고려대학교), 김성겸 (고려대학교), 홍득조 (전북대학교), 성재철 (서울시립대학교), 홍석희 (고려대학교)	
우수	국가보안기술연구소 소장상 2	스마트 홈 플랫폼 헤이홈에 대한 디지털 포렌식 아티팩트 분석 문상민, 서승희, 이창훈 (서울과학기술대학교)	학부생 우수논문
우수	한국인터넷진흥원 원장상 1	CRYSTALS-KYBER Barrett Reduction 연산에 대한 선택 암호문 공격 심보연 (한국전자통신연구원), 박애선 (군사안보지원사령부), 한동국 (국민대학교)	
우수	한국인터넷진흥원 원장상 2	자기공진 및 전자기파 무선전력전송 기술에 대한 보안위협 분석 노형준, 박기웅 (세종대학교)	학부생 우수논문
우수	한국전자통신연구원 원장상 1	바이너리 분석을 이용한 UNIX 커널 기반 File System의 TOCTOU Race Condition 탐지 방법 제안 이석원, 오희국 (한양대학교)	
우수	한국전자통신연구원 원장상 2	IoT 보안 인증 제도 기반 홈 IoT 기기 애플리케이션의 취약점 분석 및 대응책 제시 윤혜진, 김은주, 최지원, 위한샘, 이옥연 (국민대학교)	학부생 우수논문

우수논문상

구분	상장명	논문명	비고
우수	학회 우수논문상 1	5G 네트워크에서 D2D 통신을 위한 Chow-Ma 보안 프로토콜의 취약점 분석 이상민, 김지윤, 김보남, 유일선 (순천향대학교)	
우수	학회 우수논문상 2	패킷 데이터 기반 기계 학습을 통한 전력 시설 내 이상 징후 탐지 방안 연구 김준원, 최현표, 서정택 (가천대학교)	
우수	학회 우수논문상 3	안드로이드 앱 암호화 API 오용 탐지 연구 이민욱, 김은수, 오상학, 김형식 (성균관대학교)	
우수	학회 우수논문상 4	GPU 상에서의 블록암호 PIPO 병렬 구현 권혁동, 박재훈, 엄시우, 서화정 (한성대학교)	
우수	학회 우수논문상 5	적대적 공격과 커버리지 기반 딥러닝 퍼징의 유효성 비교 분석 엄주언, 박래현, 김재욱, 권태경 (연세대학교)	
우수	학회 우수논문상 6	데이터 재사용 공격에 대한 방어법 고찰 이대진, 이준오, 차상길 (한국과학기술원)	
우수	학회 우수논문상 7	분산 ID 기반 모바일 학생증 구현 조승현, 강민정, 강지윤, 이지은, 이경현 (부경대학교)	학부생 우수논문
우수	학회 우수논문상 8	SNS 애플리케이션 아티팩트 기반 보안 위협 분석 송유래, 정해선, 곽진 (아주대학교)	학부생 우수논문
우수	차세대 여성과학자 1	StyleGAN2로 생성한 얼굴 이미지 탐지 윤경은, 유하은, 이예은, 김명주 (서울여자대학교)	
우수	차세대 여성과학자 2	비트슬라이스 블록 암호에 대한 다중 신경망 프로파일링 부채널 분석-Case Study PIPO 김연재, 김수진, 한동국 (국민대학교)	
우수	차세대 여성과학자 3	이더리움 샤딩 상에서 Parallel Tabu Search를 이용한 account 재배치기법 이연주, 최재현, 정재열, 정익래 (고려대학교)	

※ 기관명은 카테고리별 가나다순

개회식

*일시 : 2021년 6월 24일(목), 11:00~12:00
*장소 : 과학기술회관 12F 아나이스홀 실시간 촬영 및 유튜브 생중계

시 간	내 용
11:00~11:30	**초청강연** **주제 : Large scale analysis on phishing attacks** 안길준 삼성전자 전무 / Arizona State University 교수
11:30~12:00	**개회식** 개회사 : 류재철 한국정보보호학회 회장 환영사 : 이동만 KAIST 공과대학 학장 **시상식** 최우수상 : 과학기술정보통신부 장관상, 행정안전부 장관상, 한국정보보호학회장상 우수상 : 국가보안기술연구소 소장상, 한국인터넷진흥원 원장상, 한국전자통신연구원 원장상, 학회장상, 차세대 정보보호여성과학기술인상

세션	발표 논문
AI 보안1	**오디오 적대적 예제 생성 시 Target Phrase 선택에 따른 Perturbation의 변화 분석** 손배훈, 문현준, 서성관, 윤주범(세종대학교)
	데이터 재복원을 통한 연합학습의 프라이버시 침해 장진혁, 최대선(숭실대학교)
	AI 예측에 대한 신뢰도 분석 연구 이은규, 김홍비, 이태진 (호서대학교)
	전이 공격에 강건한 딥러닝 모델을 위한 특징 기반 적대적 학습 류권상, 최대선(숭실대학교)
	적대적 신경망 기반의 암호 설계 기술 연구 정수용, 홍도원, 서창호 (공주대학교)
	딥러닝을 활용한 Feistel 구조에 대한 암호 모방 공격 임우상, 홍도원, 서창호 (공주대학교)
	사용자의 편리를 위한 Naive Bayes 기법을 이용한 인공지능 기반 이메일 분류 시스템 강지수, 김민지, 김하늘, 윤지인, 이현정, 김형종(서울여자대학교)

세션	발표 논문
AI 보안2	**Contour Adversarial Attack : Image의 local smoothness를 유지하기 위한 공격 기술** 나현식, 최대선(숭실대학교)
	인공지능에 적용된 양자컴퓨터 연구동향 송경주, 장경배, 심민주, 임세진, 양유진, 서화정(한성대학교)
	프라이버시 보호를 위한 Federated Learning 기반 사용자 맞춤형 광고 모델 권승주, 이소은, 최슬기, 최지희, 양대헌(이화여자대학교)
	데이터 익명화와 연합학습의 성능실험 장진혁, 최대선(숭실대학교)
	신뢰 실행환경 기반의 안전한 AI 연산 신현수, 강병훈(한국과학기술원)
	인공신경망에서의 프라이버시 보호 기법 동향 강예준, 김현지, 임세진, 김원웅, 서화정(한성대학교)
	딥러닝 공격 기법 연구 동향 : 모델 취약성을 중심으로 임세진, 양유진, 김현지, 장경배, 서화정(한성대학교)

세션

세션	발표 논문
AI 보안3	**심층 뉴럴 네트워크의 적대적 방어 기법 동향** 김재욱, 박래현, 엄주언, 권태경(연세대학교)
	적대적 공격과 커버리지 기반 딥러닝 퍼징의 유효성 비교 분석 엄주언, 박래현, 김재욱, 권태경(연세대학교)
	오디오 적대적 예제를 통한 결제 시스템 공격 사례 연구 박태정, 최태정, 하주현, 윤주범(세종대학교)
	블랙박스 환경의 Show and Tell 모델에서의 회피 공격 이동섭, 류재철(충남대학교)
	Intrusion Detection System을 회피하는 GAN 기반 적대적 CAN 패킷 생성방법 김도완, 최대선(숭실대학교)
	BERT 모델을 활용한 딥러닝기반 취약점 탐지시스템 김수린, 김형식(성균관대학교)
	스테레오 매칭 딥러닝 모델에 대한 최적화 기반 적대적 공격 심상훈(고려대학교), 주경호(고려대학교), 최원석(한성대학교), 이동훈(고려대학교)
	객체탐지모델에서의 적대적 공격 기법 연구 동향 조현진, 강효은, 김호원(부산대학교)

세션

세션	발표 논문
자동차보안1	**국제표준 기반 V2X 통신 보안취약점 분석 및 요구사항 연구** 노현정, 염흥열(순천향대학교)
	차량 내부 통신을 위한 네트워크 비교 및 보안 위협 분석 김서연, 오인수, 김찬민, 임강빈(순천향대학교)
	Ultra-Wideband 기반 측위 시스템에 대한 공격/방어기법 연구 동향 주경호 (고려대학교), 최원석 (한성대학교), 이동훈 (고려대학교)
	로드 밸런싱을 이용한 향상된 모바일 자동차 키 공유 모델 김의진, 김득훈, 곽진(아주대학교)
	SOME/IP 보안 동향 분석 강민정(한림대학교), 허재웅(숭실대학교), 김형훈(숭실대학교), 조효진(숭실대학교)

세션	발표 논문
자동차보안2	**CAN 프로토콜에서의 ECU 프레임 필터링을 통한 침입 탐지 시스템 개발** 뭉흐델게레흐, 오인수, 정소영, 임강빈(순천향대학교)
	CAN 기반 전기차 충전 프로토콜 분석 강동우 (숭실대학교), 김다영 (서울여자대학교), 신지우 (서울여자대학교), 김형훈 (숭실대학교), 주경호 (고려대학교), 조효진 (숭실대학교)
	가속도 센서를 이용한 향상된 CAN 메시지 리버스 엔지니어링 기법 정연선, 최원석 이동훈 (고려대학교)
	CAN 메시지 기반 차량 침입 탐지 시스템 분석 김형훈 (숭실대학교), 최원석 (한성대학교), 조효진 (숭실대학교)

세션

세션	발표 논문
해킹 및 취약점 분석1	**정적 오염 분석을 통한 보안 취약점 탐지** 박상희, 최진영(고려대학교)
	파이어폭스 취약점 JIT Spraying 및 Use After Free 결합 공격 윤진영, 류재철(충남대학교)
	BugClone: Towards Finding Vulnerable Source Code Clones in Binary Executables Sami Ullah, 오희국 (한양대학교)
	퍼징 기반 웹 취약점 탐지 기법 정지운, 이찬호, 황세정, 김강년, 손태식(아주대학교)
	5G-AKA 및 SMC의 RAN 취약점 분석 김태완, 김현기, 이옥연(국민대학교)

세션	발표 논문
해킹 및 취약점 분석2	**커널 블루투스 취약점을 활용한 BleedingTooth공격 분석** 정인수, 이민경, 곽진(아주대학교)
	매크로 바이러스를 통해 유포되는IcedID 유형의 악성코드 전파 방식 사례 연구 김혜민, 임정수, 최은정(서울여자대학교)
	자기공진 및 전자기파 무선전력전송 기술에 대한 보안위협 분석 노형준, 박기웅(세종대학교)
	데이터 재사용 공격에 대한 방어법 고찰 이대진, 이준오, 차상길(한국과학기술원)

세션

세션	발표 논문
IoT 보안1	**MFCC 화자 인식 기반의 사용자 인증 시스템 제안** 김정연, 김명주(서울여자대학교)
	Hyperledger Indy를 활용한 블록체인 기반 출입통제 시스템 설계에 관한 연구 강성환, 조위덕(아주대학교)
	5G 대규모 IoT 환경에서의 분산 원장을 활용한 MTD 시스템에 관한 연구 고영민, 박건량, 권태웅, 이준, 송중석(한국과학기술정보연구원 과학기술사이버안전센터)
	Shodan을 이용한 IP CCTV 보안성 자가 진단 시스템 제안 진세영, 이수련, 박지윤, 이채린, 김명주(서울여자대학교)
	영지식 증명을 활용한 실내 위치 기반 서비스의 사용자 위치 정보 보호 조욱, 김금보, 김호원(부산대학교)
	RTSP를 사용하는 IP 카메라의 영상 전송 방식 분석과, 비인가자에 의한 영상 데이터 탈취 실증 김준걸, 이진우, 남수만, 김윤정, 조경제, 박영선 (두두아이티), 이해영 (청주대학교)
	임베디드 시스템의 베어메탈 펌웨어 에뮬레이션 정확도 향상 방안 이영우, 김주환, 유지현, 윤주범(세종대학교)

세션	발표 논문
IoT 보안2	**드론을 이용한 무선 네트워크 공격 시나리오 및 가능성 실증** 김동현, 강한별, 박유나, 이민규, 염흥열(순천향대학교)
	IoT 보안 인증 제도 기반 홈 IoT 기기 애플리케이션의 취약점 분석 및 대응책 제시 윤혜진, 김은주, 최지원, 위한샘, 이옥연(국민대학교)
	5G 네트워크에서 D2D 통신을 위한 Chow-Ma 보안 프로토콜의 취약점 분석 이상민, 김지윤, 김보남, 유일선(순천향대학교)
	Security Mechanism for Preventing DDoS Attacks in SDN-Enabled Smart Agriculture Yonas Engida Gebremariam, Daniel Gerbi Duguma, Philip Virgil Astillo, Bonam Kim, Ilsun You(Soonchunhyang University)
	IoD 환경에 효율적인 온/오프라인 서명 비교 및 분석 최재현, 정익래 (고려대학교), 변진욱 (평택대학교)
	ID 기반 다중대리서명의 최신 연구 동향 및 IoD 인증 환경으로의 적용 방안 연구 신영아, 정익래 (고려대학교), 변진욱 (평택대학교)
	근거리 통신망 환경의 무선 드론 취약점 분석 진호준, 황영하, 유일선(순천향대학교)

세션

세션	발표 논문
IoT 보안3	**IoD 환경에서 경량 인증을 위한 보안성 및 효율성 분석** 선하라,정재열(고려대학교),임준호(육군3사관학교),정익래(고려대학교)
	Ultrasonic Sound를 이용한 인공지능 스피커 보호 기법 전희도, 이선우, 이동훈(고려대학교)
	32-bit 프로세서 ARM Cortex-M4에서의 PIPO 최적화 구현 곽유진, 서석충(국민대학교)
	Cowrie 허니팟을 이용한 IoT 시스템 공격자 식별 및 분석 시스템 구현 차현석, 김동현, 염흥열(순천향대학교)
	IoT 장치의 음향 센서를 활용한 사용자 장치 인증 기술 동향 분석 김가겸, 박성빈, 이연준(한양대학교)
	Choose your home: Survey on Anomaly Detection Techniques for Smart Home IoT Rustam Ismailov, 이연준 (한양대학교)
	스마트 홈 플랫폼 헤이홈에 대한 디지털 포렌식 아티팩트 분석 문상민, 서승희, 이창훈(서울과학기술대학교)
	MEMS 자이로스코프 센서값 대상 스푸핑 공격 및 진동 신호 구분 방법 조현수 (고려대학교), 최원석 (한성대학교), 이동훈(고려대학교)

세션

세션	발표 논문
네트워크보안1	**네트워크 이상 탐지를 위한 앙상블 스태킹 모델 연구** 서동찬, 김형태 (전남대학교), 유영록 (소울소프트)
	제로 트러스트 보안을 위한 사이드카 프록시 기반의 데이터 수집 방법 곽송이, 양은주, 정수환(숭실대학교)
	보안 오픈소스를 활용한 효율적인 클라우드 보안 데이터 분석 방법 연구 최두섭, 송상준(웨이커 보안연구실), 김태근(순천향대학교)
	무선 통신 기술 관련 보안 이슈 양유진, 임세진, 오유진, 서화정(한성대학교)
	IoV 환경에서 데이터 전송 속도 향상을 위한 블록 체인 기반 복합 암호 시스템 정원진, 조대호(성균관대학교)

세션	발표 논문
네트워크보안2	**병렬 처리를 통한 영지식 증명 구현** 박재훈, 권혁동, 서화정(한성대학교)
	Cuckoo Sandbox 기반 파일 악성행위 자동분석을 통한 BitTorrent 파일공유 프레임워크 차해성, 공성현, 이창훈(서울과학기술대학교)
	WPA3의 OWE를 적용한 개선된 Zigbee 인증 프로토콜 유호제, 김찬희, 이지웅, 조예림, 신은규, 임성식, 오수현(호서대학교)
	사이버 위협 인텔리전스 공유 체계 보안 메커니즘 연구 김예능, 박훈용, 김보남, 유일선(순천향대학교)
	멀티 도메인 네트워크 토폴로지 시각화 연구 류제민(에이알씨엔에스), 장범환(호원대학교)

세션	발표 논문
네트워크보안3	**크롤러를 활용한 다크웹 유출 개인정보 탐지시스템 구현에 관한 연구** 신영재, 양희성, 이주현, 염흥열(순천향대학교)
	블랙 및 화이트리스트 기반 저작권 콘텐츠 관련 URL 관리를 통한 저작권 침해 의심 사이트 탐지 기법 이태준, 김의진, 곽진(아주대학교)
	Lua 스크립트 기반 5G AKA wireshark 플러그인 제작 정서우, 장찬국, 이옥연(국민대학교)
	6G 보안을 위한 5G 코어 오픈소스 프로젝트 분석 이세윤, 위한샘, 윤승환, 이옥연(국민대학교)
	이중토큰을 이용한 효율적인 Wi-Fi 보안 프로토콜의 보안성에 관한 정형화 검증 연구 김지윤, 이상민, 유일선(순천향대학교)
	ROS 통신 무결성 검증을 위한 데이터 인증기법과 성능평가 심경민, 조해현, 이정현(숭실대학교)

세션

세션	발표 논문
부채널분석1	**CUDA 기반 병렬 처리를 통한 상관 전력 분석(CPA)의 고속 구현** 배대현, 이재욱, 하재철(호서대학교)
	임의 값 2byte를 사용하는 최적 PIPO 1차 마스킹 김현준, 심민주, 엄시우, 서화정(한성대학교)
	딥러닝 기반 논프로파일링 부채널 분석 기술 연구 동향 심민주, 김현준, 송경주, 강예준, 김원웅, 서화정(한성대학교)
	Constant-Time FrodoKEM 암호문 비교 연산에 대한 전력분석 이태호, 한재승(국민대학교), 권지훈, 이주희(삼성SDS), 김수진, 김연재, 문혜원, 안성현(국민대학교), 심보연(한국전자통신연구원), 윤효진, 조지훈(삼성 SDS), 한동국 (국민대학교)

세션	발표 논문
부채널분석2	**기계어 수준 부채널 누설 정보 분석 및 역어셈블러 구현** 배대현, 하재철(호서대학교)
	CRYSTALS-KYBER Barrett Reduction 연산에 대한 선택 암호문 공격 심보연(한국전자통신연구원), 박애선(군사안보지원사령부), 한동국(국민대학교)
	하드웨어 기반 키 관리 모듈의 부채널 공격 동향조사 김민재, 이준호, 김호원(부산대학교)
	경량 블록암호 PIPO에 대한 단일 바이트 오류 기반 차분 오류 공격 임성혁, 한재승, 이태호, 한동국(국민대학교)

세션	발표 논문
부채널분석3	**경량 블록암호 PIPO에 대한 딥러닝 기반 프로파일링 부채널 분석의 라벨별 비교** 우지은, 문혜원, 안성현, 한동국(국민대학교)
	신규 블록암호 PIPO에 대한 효율적인 상관전력분석 김수진, 안성현, 김연재, 문혜원, 우지은, 한동국(국민대학교)
	비트슬라이스 구조에 효율적인 딥러닝 기반 비프로파일링 부채널 분석 - Case Study: PIPO 한재승, 임성혁, 이태호, 한동국 (국민대학교)
	System Side Channel Information 기반 Control-flow Attack 탐지 기법 설계 및 구현 김선권, 진홍주, 이지원, 이동훈(고려대학교)

세션

세션	발표 논문
CPS 보안	**Purdue Enterprise Reference Architecture 기반 시스템 최적 배치 결정 방법론** 김경호, 김후언, 김휘강(고려대학교)
	SWaT 테스트베드 데이터셋을 활용한 비정상행위 탐지 성능 비교 황종배, 장세창, 장재원, 고성용, 하재철(호서대학교)
	패킷 데이터 기반 기계 학습을 통한 전력 시설 내 이상 징후 탐지 방안 연구 김준원, 최현표, 서정택(가천대학교)
	원전 사이버보안 훈련 시나리오 개발 방안 연구 송인성, 서정택(가천대학교), 이인효(한국원자력통제기술원)
	원자력시설 사이버 보안조치 평가 방법론 TAM과 NEI 13-10 비교 분석 정다운, 최현표, 서정택(가천대학교)

세션	발표 논문
블록체인1	**분산 ID 기반 모바일 학생증 구현** 조승현, 강민정, 강지윤, 이지은, 이경현 (부경대학교)
	블록체인 활용 비대면 전자계약 시스템 김남석, 김천구, 심민기, 이동훈, 김재수(경북대학교)
	블록체인을 이용한 소프트웨어 라이선스 관리 시스템 설계 및 구현 최성현, 박현균, 염기준, 염흥열(순천향대학교)
	블록체인 기반 프라이버시 강화 자기주권 신원증명 아키텍처 김도훈, 김동규, 오상봉, 김호원(부산대학교)
	컨텐츠 무결성을 제공하기 위한 Hashlink 기반의 안전한 DID 시스템 김태훈, 이임영(순천향대학교)
	블록체인 기반의 약품 유통 관리 시스템 연구 최재혁, 서정택(가천대학교)

세션

세션	발표 논문
블록체인2	**블록체인 기반 탈중앙형 서비스에서 공정한 부인방지 프로토콜의 보안 요구사항 분석** 조강우, 전미현, 신상욱(부경대학교)
	STRIDE 위협 모델링에 기반한 블록체인 서비스 보안성 확보 방안 윤영수(고려대학교)
	블록체인 기반 부인방지 프로토콜 비교 분석 전미현, 조강우, 신상욱(부경대학교)
	다중 식별자 캐시 리소스를 통한 DID 기반의 사일로 데이터 신뢰 협업 시스템에 관한 연구 라경진, 이임영(순천향대학교)
	분산형 의료 환경에서 넛지 이론을 적용한 환자 정의 데이터 개인 정보 보호 관리 제안 장설아, Qian Zhuoha, 이경현(부경대학교)
	A Study of Secure Edge Intelligent on Internet of Vehicle Muhammad Firdaus, Kyung-Hyune Rhee(Pukyong National University)

세션

세션	발표 논문
암호화폐	**머신러닝을 통한 비트코인 이상 거래 탐지** 권혜민, 윤명지, 이승아, 조유진, 김명주(서울여자대학교)
	이더리움 토큰표준 분석 강승주(고려대학교) ,임준호(육군3사관학교), 정익래(고려대학교)
	암호화폐 탈중앙화 거래소(DEX) 비교 및 분석 이민섭, 정익래(고려대학교)

세션	발표 논문
암호이론1	**디지털 위임 서비스에 활용 가능한 PKI 기반 권한 위임 프로토콜 제안** 고나현, 김자현, 박세란(서울여자대학교)
	검색 가능한 암호화 기술의 발전과 현재 김예은, 오희국(한양대학교)
	인증서와 전자서명을 이용하는 QR코드 기반 안심택배서비스 권현주, 신세영, 유현진, 이병천(중부대학교)
	Grover 알고리즘 적용을 위한 Simplified AES 최적 구현 장경배, 송경주, 엄시우, 심민주, 강예준, 김원웅, 서화정(한성대학교)
	Parallel implementation of lightweight block cipher PIPO using AVX2 김현지, 김현준, 엄시우, 권혁동, 서화정(한성대학교)
	Super Box의 고원 특성 분석 – 최적의 S-box 선형계층 김성겸(고려대학교), 홍득조(전북대학교), 성재철(서울시립대학교), 홍석희(고려대학교)
	증명 가능한 안전성을 가지는 아이소제니 기반 해시 함수 설계 허동희, 홍석희(고려대학교)
	8-bit AVR 환경에서 PIPO 최적 구현 김영범, 서석충 (국민대학교)

세션	발표 논문
암호이론2	**GPU 상에서의 블록암호 PIPO 병렬 구현** 권혁동, 박재훈, 엄시우, 서화정(한성대학교)
	축소 라운드 GIFT의 향상된 차분, 선형 특성 백승준, 김한기, 김종성(국민대학교)
	S-Box 구조를 활용한 Division Property 분석 연구 김제성, 김성겸(고려대학교), 홍득조(전북대학교), 성재철(서울시립대학교), 홍석희(고려대학교)
	의료 클라우드 환경에서 KP-ABE 기반의 안전한 데이터 공유시스템에 관한 연구 황용운, 이임영(순천향대학교)
	일정 수의 라운드를 가지는 무인증서 기반 인증 및 그룹키 합의 프로토콜에 관한 연구 임혜민, 이임영(순천향대학교)
	Utilization of Full y Homomorphic Encryption Technology in Healthcare Industry 홍미연, 윤지원 (고려대학교)
	블록암호의 양자회로 설계 연구 정건상, 김성겸 (고려대학교), 홍득조 (전북대학교), 성재철 (서울시립대학교), 홍석희 (고려대학교)
	확장된 RNBP 알고리즘 박종현, 전용진, 김종성(국민대학교)
	NIST PQC Round 3 Finalist 후보 KYBER NTT 곱셈에 대한 상관전력분석 김수진, 김연재, 문혜원, 안성현, 이태호, 한재승, 한동국(국민대학교)
	GPU 환경에서의 SHA-3(512) 병렬 최적 구현 최호진, 서석충(국민대학교)

세션

세션	발표 논문
암호이론3	**LAT를 이용한 S-box 구조분석** 김선엽, 김성겸(고려대학교), 홍득조(전북대학교), 성재철(서울시립대학교), 홍석희(고려대학교)
	Controlled CDKM 최적화 양자 회로 구현 전찬호, 홍석희(고려대학교)
	NTRU-HPS 키 생성 알고리즘에 대한 단일파형 기반 전력 분석 김규상, 박동준, 김희석, 홍석희(고려대학교)
	Trends of techniques for encrypted outsourcing-data 김원웅, 강예준, 이승빈, 임세진, 김현지, 박재훈, 서화정(한성대학교)
	VS2017의 성능 프로파일링을 이용한 NIST PQC Round 3 암호의 성능 분석 이명훈, 박동준, 홍석희(고려대학교)
	PQC와 QKD 기술을 활용한 최신 연구 동향 한찬희, 최여정, 이만희(한남대학교)
	비선형 로그 함수를 사용한 완전동형암호 기법에서 지수 분포의 최대 가능도 추정 유준수, 윤지원(고려대학교)
	병렬 컴퓨팅을 이용한 완전 동형암호 논리 회로 연산 시간 개선 유준수, 윤지원(고려대학교)
	RISC-V 프로세서 상에서의 경량 블록 암호 SIMON과 SPECK 최적 구현 엄시우, 권혁동, 김현지, 서화정(한성대학교)
	경량 블록암호 PIPO 기반 CTR_DRBG 분석 박서진, 김수리(성신여자대학교)

세션

세션	발표 논문
시스템보안1	**악성코드 분류 기술의 동향 및 시사점** 김준섭(이스트시큐리티, 세종대학교), 박기웅(세종대학교)
	LIME 기반 악성코드 그룹분류 해석 연구 정아연, 김도연, 김진강, 이태진 (호서대학교)
	바이너리에서 메모리 경계 복구를 통한 Out-of-bounds 취약점 탐지 유동민, 오희국(한양대학교)
	바이너리 분석을 이용한 UNIX 커널 기반 File System의 TOCTOU Race Condition 탐지 방법 제안 이석원, 오희국(한양대학교)
	바이너리에서 Invalid Memory Access 취약점 탐지 기술 동향 연구 김문희, 오희국(한양대학교)
	Themida 자동 역난독화 시스템 김민호, 조해현, 이정현(숭실대학교)
	2020년 및 2021년 국내·외 랜섬웨어 대응 정책 동향 강수진, 김수빈, 이민정, 김소람, 김종성(국민대학교)
	Tigress 난독화 도구에서 제공하는 MBA 난독화 기술의 한계점 이지원 (고려대학교), 석재혁 (삼성 SDS), 이동훈 (고려대학교)

세션	발표 논문
시스템보안2	**차등 테스트를 통한 Qualcomm Hexagon 에뮬레이터 분석** 정현식, 윤인수, 김용대(한국과학기술원)
	항공 소프트웨어 보안 인증을 위한 공통평가기준(Common Criteria) 적용방안 연구 정송희, 윤동환, 박영호(세종사이버대학교)
	항행시스템 인증을 위한 보안 인증계획서 연구 윤동환, 정송희, 박영호(세종사이버대학교)
	A Survey of Using Machine Learning to Detect Vulnerability Based on Source Code 이신계, 오희국(한양대학교)
	상용 클라우드 서비스 대상 내부 자원 모니터링 및 보안 위협 커버리지 분석 조여름, 박기웅(세종대학교)
	딥 러닝 기반의 코드 유사도 탐지 방법 동향 반영훈, 조해현, 이정현(숭실대학교)
	CodeQL 데이터베이스 생성 시 소스코드 추출 시간 분석 이소연, 윤종희(영남대학교)
	클라우드 보안 분류체계 설계를 위한 요구사항 도출 양주호, 박기웅(세종대학교)

세션	발표 논문
시스템보안3	**UAV 사고 원인 분석 기술 동향 및 사고 재현 시스템 디자인 방향성 도출** 최기철, 박기웅(세종대학교)
	중간값 참조 테이블을 활용한 CPU-GPU 하이브리드AES-XTS 최적화 기법 안상우, 서석충(국민대학교)
	OpenCL, OpenMP 병렬처리를 사용한 PIPO 알고리즘 구현 박보선, 서석충(국민대학교)
	ARMv8-A Series에서 Crystal-Dilithium Round 3의 NTT 곱셈 병렬 구현 송진교, 김영범, 서석충(국민대학교)
	보안성 및 호환성을 위한 Backward-edge Control-flow Integrity 전용 예외 처리기 설계 및 구현 진홍주, 김선권, 이동훈(고려대학교)
	차세대 보안관제 선제적 활용을 위한 SOAR 분석 이민경, 김득훈, 곽진(아주대학교)
	정적 분석 기반 OpenSSL 버전 식별 방법 김문선, 김광준, 김윤정, 이만희(한남대학교)
	시스템 소프트웨어의 이상행위 탐지 기법 심경민, 이선준, 전거창, 조해현, 이정현(숭실대학교)

세션	발표 논문
모바일보안1	**구글 디지털 웰빙 데이터를 기반으로 한 개인 맞춤 시간 관리 안드로이드 App 개발** 윤하영, 장은비(서울여자대학교)
	모바일 택배 애플리케이션 취약점 분석 지우중 (타이거 CNS), 김형기 (타이거 CNS), 김형식 (성균관대학교)
	정적오염분석을 방지하는 난독화 기법과 역난독화 방안 이동호, 조해현, 이정현 (숭실대학교)
	안드로이드 악성코드 분석을 위한 동적 애플리케이션 분석 시스템 신용구, 이선준, 조해현, 이정현(숭실대학교)
	안드로이드 어플리케이션의 개인정보 유출을 방지하기위한 민감한 데이터 흐름 보호 기법 전거창, 조해현, 이정현 (숭실대학교)

세션

세션	발표 논문
모바일보안2	**안드로이드 악성코드의 분석을 위한분석 방지 기법 조사** 김벼리, 조해현, 이정현(숭실대학교)
	정적 분석 기반 딥 러닝을 이용한 효율적인 안드로이드 멀웨어 탐지 기법 김진성, 반영훈, 고은별, 조해현, 이정현 (숭실대학교)
	안드로이드 애플리케이션들의 네이티브 코드 사용 동향 분석 최민성, 조해현, 이정현 (숭실대학교)
	안드로이드 앱 암호화 API 오용 탐지 연구 이민욱, 김은수, 오상학, 김형식(성균관대학교)
	안드로이드 패스워드 관리 어플리케이션 취약점 분석 이주현, 권지연, 홍득조(전북대학교)

세션	발표 논문
디지털 포렌식	**윈도우 환경에서 Pinngle 및 미스리 메신저 아티팩트 분석** 박귀은, 김수빈, 김현재, 이민정, 옥정수, 신수민, 김종성(국민대학교)
	iOS 백업 암호화 기술 분석 박찬규, 장진수, 류재철(충남대학교)
	적대적 예제를 이용한 스테가노그래피 이미지 윤영여, 심준석, 김호원(부산대학교)
	SNS 애플리케이션 아티팩트 기반 보안 위협 분석 송유래, 정해선, 곽진(아주대학교)
	사진 및 동영상 은닉/암호화 특정 애플리케이션 분석 최용철, 김기윤, 김종성(국민대학교)
	Active Directory 환경에서의 공격 유형 연구 김가영(고려대학교)
	카카오톡 메시지 복구 이수현, 안수빈, 김지수, 이병걸 (서울여자대학교)

세션

세션	발표 논문
사이버 정책	**중소기업 정보보호 및 개인정보보호 관리체계 연구** 김영우(고려대학교)
	무기체계 소프트웨어 보안성 확보 방안 연구 류지선, 윤경환(국방기술품질원)
	간편 ISMS 인증을 위한 핵심 보안 통제 및 축약 보안 통제 진단 가이드 툴 개발 장채연, 이동준, 염흥열(순천향대학교)
	개인정보를 취급하는 내부자 위험평가 연구 박선규(고려대학교)
	미국 NRC의 디지털계측제어시스템 변경심사 과정 분석 및 국내 원자력시설 사이버보안 심사체계 개선 고려사항 장은지(한국원자력통제기술원)
	의료 공통 데이터 모델 활성화 방안으로써 가명정보 이용에 대한 연구 주세연(고려대학교)

세션	발표 논문
여성과학자	**StyleGAN2로 생성한 얼굴 이미지 탐지** 윤경은, 유하은, 이예은, 김명주 (서울여자대학교)
	비트슬라이스 블록 암호에 대한 다중 신경망 프로파일링 부채널 분석-Case Study PIPO 김연재, 김수진, 한동국 (국민대학교)
	이더리움 샤딩 상에서 Parallel Tabu Search를 이용한 account 재배치기법 이연주, 최재현, 정재열, 정익래(고려대학교)

특별세션
학술연구 및 출판 윤리 (연구 윤리 규정을 중심으로)

학술대회 등록방법

◉ 논문모집일정

- 논문제출 마감 : 2021년 6월 4일 (금)
- 최종논문 제출 마감 : 2021년 6월 16일 (수)
- 대회 일자 : 2021년 6월 24일 (목)
- 심사결과 통보 : 2021년 6월 9일 (수)
- 발표자료(동영상) 제출 마감 : 2021년 6월 16일 (수)

◉ 등록비 및 등록방법

일반회원	일반비회원	학생회원	학생비회원
100,000원	170,000원	50,000원	80,000원

- 발표자 사전등록 마감일 : 2021년 6월 16일(수)
- 일반참가자 사전등록 마감일 : 2021년 6월 22일(화)
- 행사 종료 후, 비회원 등록자에 한하여 학회 무료 회원가입 혜택 제공
- 학회 홈페이지(www.kiisc.or.kr)에서 접속할 경우 학회행사 → 사전등록바로가기 → 학술행사 선택(2021하계학술대회)
- 학생의 경우 kiisc@kiisc.or.kr 로 학생증 사본 송부
- 학생은 다른 소속이 없는 전일제 학생(학부생 및 대학원생)에 한합니다.
- 계좌번호 : 국민은행 754-01-0008-146 (예금주 : 한국정보보호학회)
- 사전등록 시 등록비는 위의 계좌로 송금하시고, 입금자가 대리일 경우통보바랍니다.
- 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 연락 바랍니다.
- 학회 특별회원사 임직원은 학회 회원으로 준합니다.
- 홈페이지(kiisc@kiisc.or.kr) 회원광장 → 특별회원사에서 확인하실 수 있습니다.
- 등록자의 핸드폰 번호로 모바일 상품권(학술대회 기념품)이 발송될 수 있으니, 반드시 본인 핸드폰 번호를 정확하게 기재하시어 불이익이 없으시길 바랍니다.

* 입금명은 회사명으로만 기재하여 입금 시 확인이 되지 않습니다. 행사 및 등록 금액이 겹치는 경우가 있으므로 학회 입금 시 입금명은 필히 [행사명 첫 글자+ 등록자 성함]으로 기재해 주시기 바랍니다.
예) 하계학술대회 등록 홍길동 - "하홍길동" 기재

- 논문 당 최소 1명의 저자는 등록하여야 합니다