2020
한국정보보호학회 하계학술대회

CISC-S'20

Conference on Information Security
and Cryptography - Summer 2020

07.15 WED
온라인 컨퍼런스
http://www.cisc.or.kr/

주최
주관 한국정보보호학회 Korea Institute of Information Security & Cryptology

후원 국가정보원 National Intelligence Service Korea
과학기술정보통신부
행정안전부
KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY
ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute
NSR 국가보안기술연구소 National Security Research Institute
cen 아이티센 ITcen

2020
한국정보보호학회 하계학술대회

CISC-S'20

초대의 글

한국정보보호학회 회원여러분, 안녕하십니까?

1990년 학회 창립 이래 지속적으로 발전해온 한국정보보호학회 하계학술대회는 어느덧 30주년을 맞이하게 되었습니다. COVID-19 사태의 어려운 여건 속에서도 끊임없는 연구 열정을 보여주시며, 학회에 아낌없는 지원을 해주시는 모든 회원 여러분의 지대한 관심과 적극적 참여가 있었기에, 이번 하계학술대회는 COVID-19 라는 사상 초유의 팬데믹에 위축되지 않고 새로운 소통 방식의 패러다임을 향해 한 발짝 나아가기 위해 학회 창립 최초로 온라인 컨퍼런스로 개최하게 되었습니다.

이번 하계학술대회에서는 159편의 우수한 논문이 27개의 세션으로 나뉘어 온라인 발표로 진행이 됩니다. 발표될 논문들은 정보보호의 초석이라 할 수 있는 암호 분야에서부터 전통적인 컴퓨터 보안, 네트워크 보안을 다루고 있으며, 이외에도 많은 이슈가 되고 있는 블록체인, AI 보안, IoT 보안 등의 첨단 분야의 논문들도 많습니다. 특히, 연구자들의 의미있고 활발한 소통을 위해 발표되는 모든 논문 별 실시간 소통 채널을 개설하여 연구자들의 학술적 가치와 노고가 결실을 맺는 행사가 되도록 기획하였습니다. 이렇게 다양한 분야에서 탁월한 연구결과를 발표하시는 여러 회원님의 노고에 깊은 감사와 존경을 표합니다. 그리고 정보보호에 관심을 갖고 계신 모든 분들을 이번 하계학술대회에 초대하오니, 이번 대회가 토론과 친목을 도모하는 거대한 소통의 장이 되기를 기원합니다.

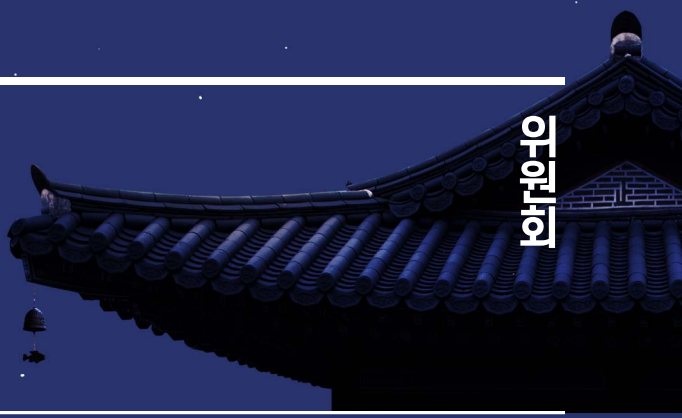
아울러 이번 학술대회를 위해 재정적으로 후원해 주신 회원사와 후원 및 협찬 기관들에게 심심한 감사를 드립니다. 또한 미래를 예측하기 힘든 상황 속에서도 하계학술대회 준비를 위해서 수고해 주신 공주대 최대선 운영위원장님과 세종대 박기웅 프로그램위원장님을 비롯한 운영 및 프로그램위원 여러분, 우리 학회 사무국 여러분께도 감사드리며 행사가 성공적으로 마무리 될 때까지 노력해 주시기를 부탁 드립니다.

이번 학술대회의 성공적인 개최를 통해 온라인 컨퍼런스의 우수 사례로 자리매김을 하고, 코로나 사태의 어려움을 전화위복의 기회로 삼아 우리나라 정보보호 산업과 기술 경쟁력이 한 차원 더 발전하는 계기가 되기를 기원합니다.
감사합니다.

2020년 7월 15일
한국정보보호학회 회장 **정 수 환**

2020
한국정보보호학회 하계학술대회

CISC-S'20



위원회

대회장 정수환 교수 (숭실대학교)

프로그램 위원회

위 원 장 박기웅 교수 (세종대학교)

위 원

곽 진 교수 (아주대학교)
김승주 교수 (고려대학교)
김형식 교수 (성균관대학교)
김희석 교수 (고려대학교)
서정택 교수 (순천향대학교)
신지선 교수 (세종대학교)
이덕규 교수 (서원대학교)
이종혁 교수 (세종대학교)
최은정 교수 (서울여자대학교)
홍득조 교수 (전북대학교)
권태경 교수 (연세대학교)
김영갑 교수 (세종대학교)
김형종 교수 (서울여자대학교)
노건태 교수 (서울사이버대학교)
서화정 교수 (한성대학교)
윤명근 교수 (국민대학교)
이만희 교수 (한남대학교)
이창훈 교수 (서울과학기술대학교)
한근희 교수 (고려대학교)
김범수 교수 (연세대학교)
김종성 교수 (국민대학교)
김호원 교수 (부산대학교)
도경화 교수 (건국대학교)
손수엘 교수 (KAIST)
윤주범 교수 (세종대학교)
이병영 교수 (서울대학교)
이태진 교수 (호서대학교)
한동국 교수 (국민대학교)
김소정 연구원 (국가보안기술연구소)
김태성 교수 (충북대학교)
김휘강 교수 (고려대학교)
박종환 교수 (상명대학교)
손태식 교수 (아주대학교)
이광수 교수 (세종대학교)
이정현 교수 (숭실대학교)
조영필 교수 (한양대학교)
허준범 (고려대학교)

운영위원회

위 원 장 최대선 교수 (공주대학교)

위 원

공준진 (삼성전자)
김정녀 (한국전자통신연구원)
도경화 (건국대학교)
손기욱 (국가보안기술연구소)
윤영태 (국가보안기술연구소)
전길수 (금융감독원)
조학수 (윈스)
홍도원 (공주대학교)
권현준 (한국인터넷진흥원)
김환국 (상명대학교)
문덕력 (한국남동발전)
송중석 (한국과학기술정보연구원)
이동휘 (동신대학교)
정현철 (정보통신기획평가원)
최두호 (한국전자통신연구원)
김익균 (한국전자통신연구원)
나재훈 (한국전자통신연구원)
문덕력 (한국남동발전)
신대규 (한국인터넷진흥원)
이상만 (시스메이트)
정현철 (인비즈넷)
최영철 (에스지에이솔루션즈)
김인중 (국가보안기술연구소)
노건태 (서울사이버대학교)
박희운 (한국인터넷진흥원)
신원 (동명대학교)
이석래 (한국인터넷진흥원)
조원석 (엘지유플러스)
한은혜 (에스에스앤씨)

2020
한국정보보호학회 하계학술대회

CISC-S'20

학술대회 등록 방법

논문 모집 일정

논문제출 마감: 2020년 6월 14일 (일)
심사결과 통보: 2020년 6월 22일(월)
최종본 제출 마감: 2020년 6월 30일(화)
발표자료(동영상) 제출 마감: 2020년 7월 6일(월)
대회 일자: 2020년 7월 15일(수)

등록비 및 등록 방법

- 학회 홈페이지(www.kiisc.or.kr)에서 접속할 경우
  학술행사 → 학회행사 → 사전등록 바로가기 → 학술행사 선택(2020 하계학술대회)
- 학생의 경우 kiisc@kiisc.or.kr 로 학생증 사본 송부
- 계좌번호 : 국민은행 754-01-0008-146 (예금주 : 한국정보보호학회)
- 사전등록 시 등록비는 위의 계좌로 송금하시고, 입금자가 대리일 경우 통보바랍니다.
- 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.
- 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.

일반회원	일반비회원	학생회원	학생비회원
200,000원	250,000원	100,000원	120,000원

* 금번 학술대회는 현장 등록이 없습니다.

2020
한국정보보호학회 하계학술대회

CISC-S'20

우수논문상

구분	상장명	(논문번호) 저자
최우수	과기부장관상	11. 양자회로에 적합한 GF(2^8) inversion 하드웨어 설계 정도영, 이승광, 최두호 (한국전자통신연구원)
최우수	행안부장관상	148. Mixcolumns의 확산 형태를 고려한 차분 확률 상한 계산 방법 김선엽, 김성겸 (고려대학교), 홍득조 (전북대학교), 성재철 (서울시립대학교), 홍석희 (고려대학교)
최우수	학회 최우수논문상 1	141. SVM 기계학습을 통한 스마트 홈 비정상 행위 탐지 기법 연구 윤건, 정재민, 허재준, 박훈용, 유일선 (순천향대학교)
최우수	학회 최우수논문상 2	109. 마이크로 컨트롤러 소비 전력 기반 명령어 수준 역어셈블러 구현 배대현, 하재철 (호서대학교)
우수	KISA 원장상 1	137. 저작권 침해 의심 사이트의 생애주기 단계 자동 탐지 기법 정해선, 곽진 (아주대학교)
우수	KISA 원장상 2	41. 양자 컴퓨팅 환경에서 안전한 다중 서명 기법 이영경 (고려대학교), 박종환 (상명대학교), 이광수 (세종대학교), 이동훈 (고려대학교)
우수	ETRI 원장상 1	140. N-gram 알고리즘을 이용한 Spectre 공격 바이너리 정적 식별 방법 김문선, 양희동, 김광준, 이만희 (한남대학교)
우수	ETRI 원장상 2	23. LTE 무선 구간 유니캐스트 메시지 인젝션을 통한 강제 가짜 기지국 연결 공격 박철준. 배상욱, 손민철, 이지호, 김홍일, 윤석빈, 황영빈, 김용대 (한국과학기술원)
우수	NSR 소장장 1	92. NIST Round 2 후보 격자 기반 KEM NTRU LPRime에 대한 신규 단일 파형 공격 심보연, 한재승, 이태호, 김일주, 한동국 (국민대학교)
우수	NSR 소장장 2	114. 클라우드 오케스트레이션 기반 침입인지형 Active-Decoy 시스템 디자인 주재경, 박기웅 (세종대학교)

우수논문상

구분	상장명	(논문번호) 저자
우수	학회 우수논문상 1	143. Simon's Algorithm을 활용한 MISTY 구조의 양자 구별자에 관한 연구 정건상, 김성겸, 홍석희 (고려대학교)
우수	학회 우수논문상 2	138. MAVLink v2 프로토콜의 암호학적 취약점 분석 김태완, 이세윤, 정서우, 위한샘, 이옥연 (국민대학교)
우수	학회 우수논문상 3	100. DBI기반 모바일 네이티브 코드 분석방지 우회 시스템 설계 신용구, 이정현 (숭실대학교)
우수	학회 우수논문상 4	81. 블록체인 기반의 전자투표 시스템에 관한 연구 송효진, 김태훈, 이임영 (순천향대학교)
우수	학회 우수논문상 5	73. 차분 프라이버시를 만족하는 안전한 재현 데이터 생성 기술 연구 정수용, 강준영, 홍도원, 서창호 (공주대학교)
우수	학회 우수논문상 6	70. 안드로이드 저장소 취약점을 이용한 악성 Application 구현 김민규, 박정수, 심현석, 정수환 (숭실대학교)
우수	학회 우수논문상 7	15. 딥러닝 시스템 커버리지 기반 퍼징 프레임워크 최적화 연구 유지현, 문현준, 윤주범 (세종대학교)
우수	학회 우수논문상 8	2. 12라운드 RECTANGLE-80에 대한 DLCT를 이용한 차분-선형 공격 조세희, 백승준, 김종성 (국민대학교)
우수	차세대여성과학자 1	30. OpenWrt를 활용한 ARP Spofing 탐지용 IDS 정연선, 김형훈, 강민정, 조효진 (한림대학교)
우수	차세대여성과학자 2	43. 국내 딥페이크 기술 현황 및 제도적 대응방안 연구 전소원, 강준형, 황진희, 우사이먼성일 (성균관대학교)
우수	차세대여성과학자 3	49. 개인정보보호를 강화한 택배 시스템 구축 노경후, 이여진, 최은정 (서울여자대학교)

2020
한국정보보호학회 하계학술대회

CISC-S'20
온라인 컨퍼런스

전체일정표

시간	내용
11:00 ~ 11:30	**초청강연** **보안 개발자로서의 삶:** 알약이 만들어지기까지 이스트시큐리티 (김준섭 부사장)
	개회식 사 회: 박기웅 교수(세종대) 개회사: 한국정보보호학회 정수환 학회장
11:30 ~ 12:00	**축사** 한국정보보호학회 남길현 명예회장 국가보안기술연구소 조현숙 소장
	시상식 최우수상: 과학기술정보통신 장관상, 행정안전부 장관상, 학회최우수논문상 우 수 상: 국가보안기술연구소 소장상, 한국인터넷진흥원 원장상, 한국전자통신연구원 원장상, 학회우수논문상 차세대 정보보호여성과학기술인상

CISC-S'20

구두발표트랙

세부일정표

발표 논문	
IoT보안	**IoT 서비스 환경에서 부인 방지를 강화하기 위한 Certificateless Signcryption에 관한 연구** 이대휘, 이임영 (순천향대학교)
	FIDO2 프로토콜을 이용한 무인택배보관함 서비스 설계 진혜윤, 강민지, 염흥열 (순천향대학교)
	스마트 홈 환경에서 Knn Algorithm을 활용한 침입탐지 기법연구 정재민, 유일선, 김보남 (순천향대학교)
	EOS 블록체인 기반 IoT디바이스 펌웨어 위변조 탐지 시스템 권현경, 김소연, 이아현, 나예원, 김형종 (서울여자대학교)
	UART를 이용한 VxWorks 쉘 권한 획득 기법 임한울, 윤주범 (세종대학교)
	SVM 기계학습을 통한 스마트 홈 비정상 행위 탐지 기법 연구 윤건, 정재민, 허재준, 박훈용, 유일선 (순천향대학교)
발표 논문	
디지털포렌식	**디지털 증거능력 측정에 관한 연구** 김영준 (아주대학교)
	윈도우에서 ZIP 파일 생성 프로그램 추정 기법 엄민지, 한재혁, 이상진 (고려대학교)
	Huawei Health 애플리케이션 아티팩트 분석 김원일, 김현재, 김수빈, 이민정, 신수민, 김종성 (국민대학교)
	책임 공유 모델을 반영한 클라우드 SOC의 포렌식 컴플라이언스 장환 (한국방송통신대학교)
	키워드 기반의 디지털 증거 탐색 유동민, 오희국 (한양대학교)
발표 논문	
자동차보안	**지속적 통합 도구 Jenkins를 이용한 보안 스택 성능 측정 및 기록 자동화** 기정은(아우토크립트 모빌리티 연구소), 김태화(포항공과대학교), 김덕수, 이정원, 한준혁, 이진우(아우토크립트 모빌리티 연구소)
	SCMS에서 버터플라이 키 확장 알고리즘의 효율성 증대 기법 최현민(아우토크립트 모빌리티 연구소), 이준석(포항공과대학교), 김의석, 주기호(아우토크립트 모빌리티연구소), 곽권구(펜타시큐리티시스템), 한준혁, 이진우(아우토크립트 모빌리티 연구소)
	CAN 데이터 분석 기술 동향 김형호, 정연선, 조효진 (한림대학교)
	머신 러닝을 이용한 자동차용 침입 탐지 이동관, 김연우 (고려대학교)
	CAMP 분석을 활용한 OBE의 보안성 평가항목 연구 김학준, 지청민, 홍만표 (아주대학교)

발표 논문	
모바일 시스템 보안	**안드로이드 저장소 취약점을 이용한 악성 Application 구현** 김민규, 박정수, 심현석, 정수환 (숭실대학교)
	DBI기반 모바일 네이티브 코드 분석방지 우회 시스템 설계 신용구, 이정현 (숭실대학교)
	Design of Anti-Analysis Evasion System Based on Method Hooking on Android 이선준, 이정현 (숭실대학교)
	Android 어플리케이션의 권한 남용 탐지에 사용된 기계학습 및 자연어 처리 기술 동향 분석 이원석, 오희국 (한양대학교)
	시스템 모니터링 기법을 통한 UAV Stealthy-Monitoring 플랫폼 디자인 최기철, 박기웅 (세종대학교)
	LTE 무선 구간 유니캐스트 메시지 인젝션을 통한 강제 가짜 기지국 연결 공격 박철준. 배상욱, 손민철, 이지호, 김홍일, 윤석빈, 황영빈, 김용대 (한국과학기술원)
	Zero-effort Applicable: 개발자 인식 없이 TEE 기반의 안전한 데이터 저장이 가능한 커스텀 안드로이드 운영체제 심현석, 윤재현, 차오녹투, 응웬휘황, 정수환 (숭실대학교)

발표 논문	
보안취약점	**SDN 웹 인터페이스를 대상으로 한 CSRF 취약점 탐지 방법** 위성일, 이현주, 손수엘 (한국과학기술원)
	MAVLink v2 프로토콜의 암호학적 취약점 분석 김태완, 이세윤, 정서우, 위한샘, 이옥연 (국민대학교)
	바이너리 취약점 탐색 성능향상을 위한 프로그램 제어문 분석 기술 연구 손기종, 김태은, 장대일, 김도원 (한국인터넷진흥원)
	챗봇의 SQL인젝션 취약점과 대응방안 연구 김태현, 박지환 (고려대학교)
	Android App에 대한 OWASP MSTG 기반 자동 분석 오호균 (고려대학교)
	Evil Twin AP와 Captive Portal을 이용한 피싱 공격 및 대응방안 연구 황선홍, 엄익채 (전남대학교)
	바이너리 레벨 Use-After-Free 취약점 탐지 기술 동향 분석 김문회, 오희국 (한양대학교)
	하이브리드 퍼저 시드 스케줄링 메커니즘 동향 권순홍(세종대학교), 최양서(한국전자통신연구원), 이종혁(세종대학교)

CISC-S'20

구두발표트랙

세부일정표

발표 논문	
악성코드	**IoT 미라이 봇넷 악성코드 정적분석** 박성범, 김경곤 (고려대학교)
	Variational AutoEncoder를 활용한 악성코드 중요 특징 추출 연구 이영전, 한명묵 (가천대학교)
	딥러닝 모델을 이용한 악성코드 탐지 방법 분석 및 비교 송어진, 고현희, 염흥열 (순천향대학교)
	악성코드 발현의 한계점을 극복하기 위한 Dynamic Binary Modification 활용 모델 제안 한찬희, 이만희 (한남대학교)
	GRU를 활용한 악성코드 탐지의 관한 연구 류경근, 이덕규 (서원대학교)
	Entry Point를 활용한 머신러닝 기반 악성코드 분석연구 김세진, 김효식, 이태진 (호서대학교)
	랜섬웨어의 심층적 이해와 중소 기업의 랜섬웨어 대처법 제안 장채연, 염흥열 (순천향대학교)
	BinDiff: Towards Semantic Aware Binary Diffing Sami Ullah, 오희국 (한양대학교)
발표 논문	
프라이버시	**Mask R-CNN 기반 개인정보보호 시스템** 박서은, 옥해림, 이수경, 최은정 (서울여자대학교)
	빅데이터의 활용과 개인정보 보호 동향 이정현, 서화정 (한성대학교)
	프라이버시 보호를 위한 무인증서 브로드캐스트 프록시 재암호화 김원빈, 이임영 (순천향대학교)
	블록체인 익명성을 이용한 인공신경망 기반 암호키 교환에서의 사용자 인증에 관한 연구 노시완, 이경현 (부경대학교)
	Consortium Blockchain에서의 프라이버시 향상을 위한 One Time Key 사용 및 검증 효율성에 관한 연구 라경진, 이임영 (순천향대학교)

	발표 논문
블록체인 1	**블록체인 기반의 복합기 관리 솔루션** 곽도훈, 라경진, 이임영 (순천향대학교)
	블록체인 기반의 전자투표 시스템에 관한 연구 송효진, 김태훈, 이임영 (순천향대학교)
	학생회비의 투명성 제고를 위한 블록체인 기반의 회계 감사 시스템 이경현, 김건오, 김민혁, 김선균, 이소연, 노시완 (부경대학교)
	블록체인 기반 스마트 컨트랙트 방식을 통한 스마트시티 내 탄소 크레딧 거래 방식 박준범, 장성주 (한국과학기술원)
	Blockchain-empowered for Secure Data Storage and Sharing in Vehicular Edge Computing Networks Firdaus Muhammad, 이경현 (부경대학교)
	허가형 블록체인을 활용한 자기 주권형 신원의 디지털 공공 · 민간서비스 플랫폼 융합 방안 조강우, 정병규, 신상욱 (부경대학교)
	발표 논문
블록체인 2	**무결성을 보장하며 보상체계를 갖는 블록체인 기반 커뮤니티 정보교류 Web 환경** 윤혜원, 김원희, 김다영, 노혜윤, 김형종 (서울여자대학교)
	블록체인 네트워크 한계 보완을 위한 사이드체인 동향 심민주, 최승주, 서화정 (한성대학교)
	Secure Localized Training in Collaborative Learning Schemes Rahmadika Sandi, 이경현 (부경대학교)
	블록체인에서 랜덤 비콘 프로토콜을 이용한 PRNG 비교 분석 정병규, 조강우, 신상욱 (부경대학교)
	사물 인터넷 환경에서 수정 가능한 블록체인 기반 접근제어 시스템 설계 임준호 (고려대학교), 천지영 (이화여자대학교), 노건태 (서울사이버대학교), 정익래 (고려대학교)
	IoT 환경에서의 블록체인 활용에 대한 연구 김대영, 이덕규 (서원대학교)
	발표 논문
어플리케이션 보안	**암표방지를 위한 모바일 티켓팅 시스템에 관한 연구** 송윤민, 황용운, 이임영 (순천향대학교)
	하이퍼레저 패브릭 기반 장학금 통합 관리 시스템 개발 김은별, 송경린, 최찬미, 최윤영, 채기준 (이화여자대학교)
	회전에 강한 특징을 이용한 돌로네 기반 대체 가능 지문 템플릿 연구 이민섭, 이상훈, 정익래 (고려대학교)
	암호화 API 오용 탐지에 관한 연구 동향 조사 이민욱, 조금환, 김형식 (성균관대학교)
	Zero-Knowledge Proof 기반의 마이데이터 서비스 제공 방안 이민경, 최슬기, 곽진 (아주대학교)

	발표 논문
산업보안	IEC 62443-4-2 기반 HVDC 및 ESS 보안 적용 방안 박원경 ((주)효성)
	SCADA 시스템에 대한 랜섬웨어 최신 동향 분석 조서연, 서승희, 조민정, 이창훈 (서울과학기술대학교)
	안전한 원격 근무를 위한 그룹키 기반 프로토콜 제안 김의진, 김득훈, 곽진 (아주대학교)
	몬테카를로 시뮬레이션을 통한 기업의 위험표현 및 사이버보험 효과도 분석 연구 김민수, 김예주, 왕성진, 김형종 (서울여자대학교)
	발표 논문
해킹 및 방어 기술	안드로이드 UI 은닉을 통한 소프트웨어 기반 카메라 프레임 탈취 기법 한수민, 심현석, 박정수, 정수환 (숭실대학교)
	키보드 입력 감지 트리거 구현 및 분석 박연균, 윤종희 (영남대학교)
	Python Pickle 모듈을 통한 쉘코드 Exploitation과 Mitigation 연구 윤창조, 김경곤 (고려대학교)
	N-gram 알고리즘을 이용한 Spectre 공격 바이너리 정적 식별 방법 김문선, 양희동, 김광준, 이만희 (한남대학교)
	Federated Learning에서 개선된 백도어 공격 방법 임규민, 김창진, 서재홍 (한양대학교)
	안티바이러스의 자가 보호 기법 분석 이성원, 윤종희 (영남대학교)
	발표 논문
암호 알고리즘 1	Multi-Client 환경에서 Forward Security를 보장하는 검색 암호 동향 분석 한창희, 허준범 (고려대학교)
	Grover's Algorithm을 통한 S-DES 공격 기법 이상헌, 조민규 (고려대학교)
	Simon's Algorithm을 활용한 MISTY 구조의 양자 구별자에 관한 연구 정건상, 김성겸, 홍석희 (고려대학교)
	Application of Neural Network Differential Distinguisher on SIMON-32/64 Erzhena Tcydenova, 조민정, 석병진, 이창훈 (서울과학기술대학교)

	발표 논문
암호 알고리즘 2	**DLCT를 적용한 PRESENT 축소 라운드 분석** 이종혁, 박종현, 백승준, 김종성 (국민대학교)
	전방향 안전성를 보장하는 공개키 기반 키워드 검색 한창희, 허준범 (고려대학교)
	전방향 안전성을 가지며 프레임 공격에 안전한 래티스 기반 그룹 서명 김준식 (고려대학교), 박종환 (상명대학교), 이광수 (세종대학교), 이동훈 (고려대학교)
	재암호화를 이용한 캡슐화 기반의 키 복구 시스템 김태훈, 김원빈, 이임영 (순천향대학교)
	Neural Linear Cryptanalysis 기법을 적용한 DES 분석 김동훈, 권동근 (고려대학교), 김성겸 (고려대학교), 홍득조 (전북대학교), 성재철 (서울시립대학교), 홍석희 (고려대학교)
	발표 논문
암호 알고리즘 3	**12라운드 RECTANGLE-80에 대한 DLCT를 이용한 차분-선형 공격** 조세희, 백승준, 김종성 (국민대학교)
	효과적인 자원관리를 위한 적응형 암호 알고리즘 연구:키 블록 생성에 대한 개선을 중심으로 김지윤, 이상민, 유일선 (순천향대학교)
	차분 프라이버시를 만족하는 안전한 재현 데이터 생성 기술 연구 정수용, 강준영, 홍도원, 서창호 (공주대학교)
	Mixcolumns의 확산 형태를 고려한 차분 확률 상한 계산 방법 김선엽, 김성겸 (고려대학교), 홍득조 (전북대학교), 성재철 (서울시립대학교), 홍석희 (고려대학교)
	인텔 SGX를 활용한 검색 가능한 암호 기법의 연구 동향 윤현도, 허준범 (고려대학교)
	발표 논문
사이버공방훈련	**사이버 보안 훈련을 위한 화이트리스트 기반 방어 에이전트에 대한 연구** 서성연, 김동화 (국방과학연구소), 안명길 (국방과학연구소, 중앙대학교)
	CTFv : 관전 가능한 공방 훈련 CTF 플랫폼 정재우, 곽지훈, 권승필, 장세정, 박기웅 (세종대학교)
	IDS/IPS 장비를 이용한 공격/방어 시나리오 기반 네트워크 보안 실습교육 환경구축 김민주, 문은실, 김형종 (서울여자대학교)

	발표 논문
모바일 앱 보안	**국내 안드로이드 게임 보호기법 분석** 김원겸 (동양대학교), 이헌 (가천대학교), 김재환 (가천대학교), 김주성 (세종대학교), 임민정 (서울과학기술대학교), 최준호 (백석대학교)
	역분석을 통한 WhatsApp의 상세 암호 동작 과정 분석 박선영, 김경곤 (고려대학교)
	배달앱 신뢰성 강화 방법에 대한 연구 권용빈, 김현지, 심민주, 서화정 (한성대학교)
	안드로이드 랜덤채팅 및 화상회의 어플리케이션 취약점 분석 방법론에 대한 연구 이용화, 최원석, 백승훈 (고려대학교)
	클라우드 파일 공유 환경에 활용 가능한 속성기반암호 기반 파일 보호 안드로이드 App 개발 신희서, 최성은, 김형종 (서울여자대학교)
	적대적 공격에 견고한 Perceptual Ad-Blocking 디자인 김민재, 김보민, 허준범 (고려대학교)
	발표 논문
AI보안	**DNN 모델 취약점 적대적 예제 생성 기법과 방어기법에 대한 분석** 서성관, 문현준, 윤주범 (세종대학교)
	딥러닝 시스템 커버리지 기반 퍼징 프레임워크 최적화 연구 유지현, 문현준, 윤주범 (세종대학교)
	Variant AutoEncoder 기반 모바일 맬웨어 클러스터링 기법 고은별, 김진성, 반영훈, 이정현 (숭실대학교)
	딥러닝을 활용한 CCTV 내 폭력 탐지 시스템 개발 김태옥, 박현아, 임다연, 최은정 (서울여자대학교)
	머신러닝 기반 네트워크 트래픽 분석 기법 성능 비교 황종배, 하재철 (호서대학교)
	금융데이터를 활용한 연합학습 평가 장진혁, 최대선 (공주대학교)
	CNN을 이용한 스마트 폰 부채널 공격 김동현, 김지은, 유건우, 이승대, 백유진 (우석대학교)
	K-means Clustering을 이용한 kNN 속도개선에 관한 연구 김도연, 이용수, 윤재헌, 이태진 (호서대학교)

CISC-S'20

구두발표트랙

세부일정표

발표 논문	
신원/인증 시스템	**분산 ID 기반 비대면 데이터 공유 접근 시스템** 이정륜, 윤태연 (블록체인기술연구소), 이우기 (인하대학교)
	차세대 주민등록정보시스템 구축에 대한 연구 이현철, 김대영 (대신정보통신㈜), 김현수 (한국지역정보개발원)
	탈 중앙화된 분산 ID 시스템의 특징 및 한계에 대한 동향 조사 이길희 (성균관대학교), 김석현 (한국전자통신연구원), 김은수, 전소원 (성균관대학교), 김봉곤 (한국뉴욕주립대학교), 조영섭 (한국전자통신연구원), 이호준, 우사이먼성일, 김형식 (성균관대학교)
	열 기반 슬라이싱을 이용한 폐기 가능한 홍채 템플릿 생성 방법 신영아, 정재열, 정익래 (고려대학교)
	안면인식을 통한 USB 파일 복호화 시스템 송경주, 강혜진, 백민진, 김현지, 서화정 (한성대학교)
	스마트폰과 스마트워치를 활용한 2차 사용자 인증 방식 제안 심민주, 엄시우, 김현지, 서화정 (한성대학교)
발표 논문	
암호화폐/ 양자암호	**암호화폐 금전가치 분석 동향** 박재훈, 최승주, 서화정 (한성대학교)
	암호화폐 거래 믹싱을 통한 익명화기술 동향조사 장설아, 이경현 (부경대학교)
	스마트 컨트랙트의 동적 모니터링을 지원하는 이더리움 가상머신 김지수, 이수연, 조은선 (충남대학교)
	NIST 양자내성암호 공모전 부호 기반 암호 구현 동향 최승주, 김현지, 심민주, 서화정 (한성대학교)
	양자 컴퓨팅 환경에서 안전한 다중 서명 기법 이영경 (고려대학교), 박종환 (상명대학교), 이광수 (세종대학교), 이동훈 (고려대학교)
	μ-Hope : 오류 정정 부호를 사용한 RLWE 기반 KEM 이주엽, 김수리, 홍석희 (고려대학교)

	발표 논문
데이터식별/추적	**저작권 침해 의심 사이트의 생애주기 단계 자동 탐지 기법** 정해선, 곽진 (아주대학교)
	링크분석 기반 영상 저작권 침해 스트리밍 사이트 탐지 방안 이희승, 곽진 (아주대학교)
	스팸 리뷰 판별을 위한 텍스트 분석 관련 기술 동향 임세진, 김현지, 서화정 (한성대학교)
	음란물 유포 경로 추적을 위한 Tumblr 애플리케이션 메모리 포렌식 분석 박진성, 공성현, 이창훈 (서울과학기술대학교)
	안드로이드 어플리케이션의 DRM 기술 현황 분석 : 카카오멜론, 카카오톡 이나연, 김도연, 양승욱, 김희석 (고려대학교)
	메시지 시그니처 분석을 통한 송신자 식별 방안 김동현, 곽진 (아주대학교)
	발표 논문
사이버정책/침해대응	**디지털 장의 유형 분석과 법적 기반 연구** 이태준, 김경곤 (고려대학교)
	한국 사이버공격 심각도 산정방안 연구 유영인, 배선하, 이종태 (한국전자통신연구원 부설연구소)
	정부의 스마트 업무환경으로의 전환에 따른 사이버보안 정책에 관한 연구 - 미국 연방 IT 현대화 정책 추진사례를 중심으로 김동희, 김소정 (한국전자통신연구원 부설연구소)
	글로벌 클라우드 컴퓨팅 보안 인증제도 비교 분석 및 국내 인증 기준 개선방안 유경아, 송인성, 염흥열 (순천향대학교)
	분산 ID 플랫폼에서의 GDPR 준수 여부 탐구 전소원 (성균관대학교), 김석현 (한국전자통신연구원), 이길희 (성균관대학교), 김봉곤 (한국뉴욕주립대학교), 조영섭 (한국전자통신연구원), 이호준, 김형식 (성균관대학교), 우사이먼성일 (성균관대학교)
	데브옵스와 대용량 로그 수집을 활용한 침해사고 대응 자동화 기법 연구 박건호, 유안지 (한국외국어대학교)

CISC-S'20

구두발표트랙

세부일정표

	발표 논문
클라우드보안	**클라우드 오케스트레이션 기반 침입인지형 Active-Decoy 시스템 디자인** 주재경, 박기웅 (세종대학교)
	컨테이너 이미지 취약점 분석 도구에 대한 분석과 비교 나한일, 응웬부렁, 단티엔북, 정수환 (숭실대학교)
	Immortal Cloud Service 제공을 위한 요구 사항 도출 김성진, 최상훈, 박기웅 (세종대학교)
	안전한 클라우드 서비스 제공을 위한 보안 위험요소 및 아키텍처 분석 김동영 (세종사이버대학원)
	서명 기반의 검증 가능 아웃소싱 제공되는 CP-ABE 기반의 데이터 공유시스템에 관한 연구 황용운, 이임영 (순천향대학교)
	스마트시티에서 클라우드 컴퓨팅을 활용한 사이버 위협 인텔리전스 공유 모델 연구 박훈용, 허재준, 유일선 (순천향대학교)
	발표 논문
부채널분석 1	**부채널 정보 기반 디어셈블리 동향** 김현준, 서화정 (한성대학교)
	NIST Round 2 후보 마스킹된 qTESLA 전자서명 알고리즘에 대한 단일 파형 공격 김일주, 심보연, 이태호, 한재승, 한동국 (국민대학교)
	ChipWhisperer 부채널 분석 소프트웨어 분석 및 비교 권혁동, 심민주, 임세진, 서화정 (한성대학교)
	신규 AES 함수 생략 오류 주입 공격 김주환, 이종혁, 한동국 (국민대학교)
	CPU 환경에서 병렬처리를 통한 PBKDF2-HMAC-LSH256 최적화 연구 최호진, 서석충 (국민대학교)
	계층형 결정적 지갑에 대한 부채널 공격 시나리오 박동준, 김희석, 홍석희 (고려대학교)
	AES H/W 구현기법에 대한 TVLA 안전성 검증 문재근, 이태호 (국민대학교), 백유진 (우석대학교), 한동국 (국민대학교)
	자바스크립트 환경에서 경량암호 CHAM-64/128 최적화 연구 박보선, 서석충 (국민대학교)

CISC-S'20

구두발표트랙

세부일정표

	발표 논문
부채널분석 2	**카라추바 곱셈 양자회로 구현 동향** 장경배, 최승주, 심민주, 서화정 (한성대학교)
	8-bit AVR 환경에서 CTR_DRBG 난수 발생기 최적화 연구 김영범, 서석충 (국민대학교)
	NIST Round 2 후보 LAC Key Encapsulation Mechanism에 대한 신규 단일 파형 공격 이태호, 심보연, 김일주, 한재승, 한동국 (국민대학교)
	다중 작업 학습을 이용한 딥러닝 기반 부채널 분석 연구 진성현, 김희석, 홍석희 (고려대학교)
	AVX2를 이용한 리자뭉 구현 권영빈, 권혁동, 김현지, 서화정 (한성대학교)
	양자회로에 적합한 GF(2^8) inversion 하드웨어 설계 정도영, 이승광, 최두호 (한국전자통신연구원)
	16-bit MSP430 환경에서 GCM의 GHASH 함수 최적화 구현 이지원, 서석충 (국민대학교)
	이종(異種) 오류원을 사용한 다중 오류 주입 시스템 이종혁, 한동국 (국민대학교)
	발표 논문
부채널분석 3	**부채널 분석 기반 랜섬웨어 대응책 동향** 김현지, 임세진, 서화정 (한성대학교)
	랜덤 워드 오류 기반 향상된 LEA 차분 오류 공격 임성혁, 이종혁, 한동국 (국민대학교)
	ARMv8에서 ASIMD 명령어를 이용한 HIGHT 암호 최적화 연구 송진교, 서석충 (국민대학교)
	화이트 박스 암호에 대한 단순 계산 분석 기법 이예찬, 김희석, 홍석희 (고려대학교)
	NIST Round 2 후보 격자 기반 KEM NTRU LPRime에 대한 신규 단일 파형 공격 심보연, 한재승, 이태호, 김일주, 한동국 (국민대학교)
	마이크로 컨트롤러 소비 전력 기반 명령어 수준 역어셈블러 구현 배대현, 하재철 (호서대학교)
	결정론적 난수발생기 CTR_DRBG의 병렬 최적화 연구 안상우, 서석충 (국민대학교)
	비트슬라이스 구현 블록암호에 대한 효율적 상관전력분석 기법 한재승, 김수진, 김연재, 심보연, 한동국 (국민대학교)

구두발표트랙

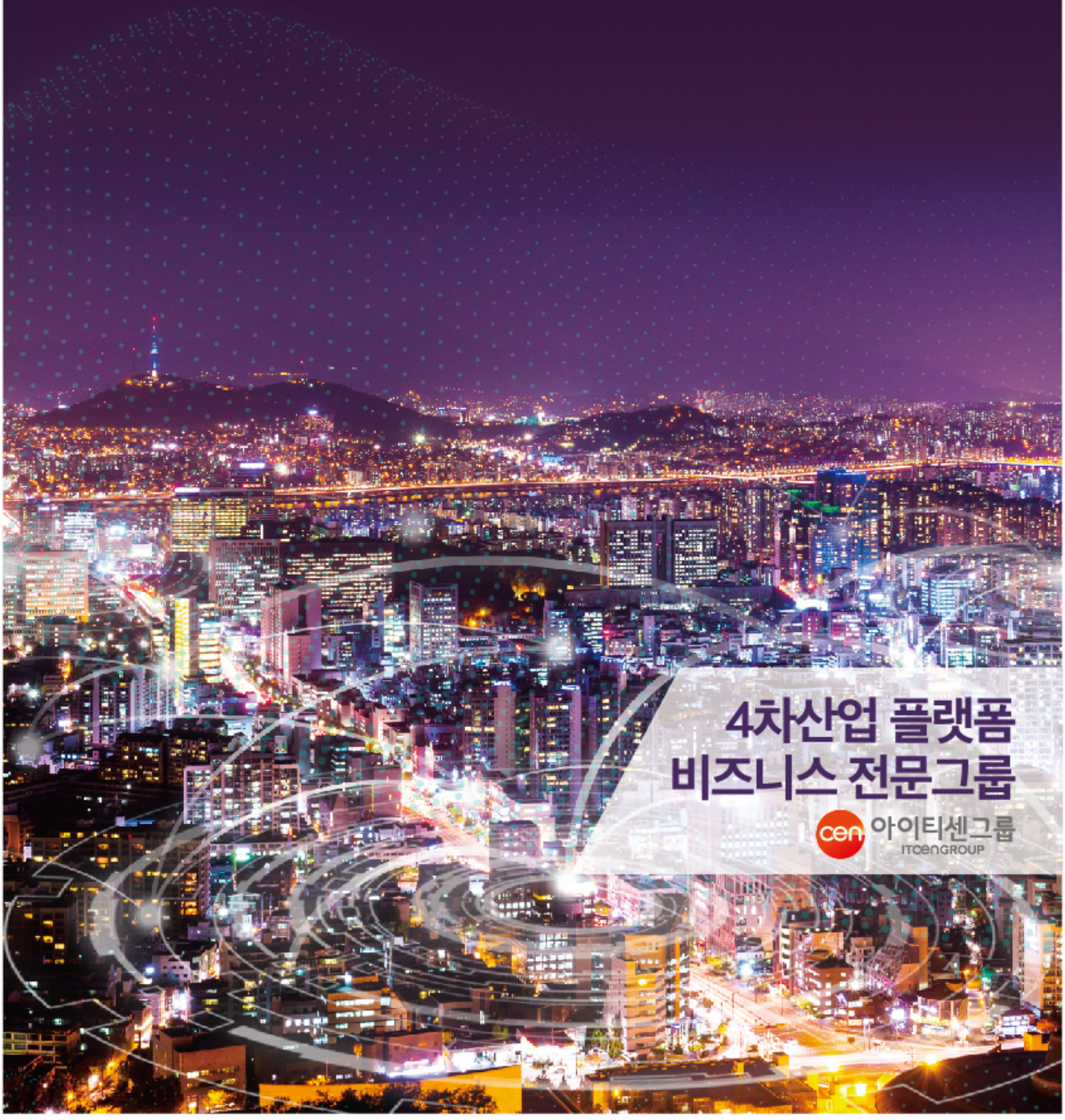
CISC-S'20

세부일정표

	발표 논문
여성과학자	**OpenWrt를 활용한 ARP Spofing 탐지용 IDS** 정연선, 김형훈, 강민정, 조효진 (한림대학교)
	국내 딥페이크 기술 현황 및 제도적 대응방안 연구 전소원, 강준형, 황진희, 우사이먼성일 (성균관대학교)
	개인정보보호를 강화한 택배 시스템 구축 노경후, 이여진, 최은정 (서울여자대학교)
	[초청강연] "블록체인 표준화 동향 및 보안" 오경희 대표 (TCA Services)

당신이 오늘 만날 수 있는 혁신

Innovation & Reality



4차산업 플랫폼 비즈니스 전문그룹

cen 아이티센그룹 ITCENGROUP

cen 아이티센 KOSDAQ | cen 소프트센 KOSDAQ | cen 굿 | KONEX 센 | cen 시 큐 KONEX 센 | comtec (주)콤텍시스템 KOSPI | comtec (주)콤텍정보통신 비상장 | KOREA GOLD EXCHANGE 한국금거래소 비상장