한국정보보호학회
Korea Institute of Information Security & Cryptology

2020년 한국정보보호학회 동계학술대회

CISC-W'20

Conference on Information Security and Cryptography-Winter 2020

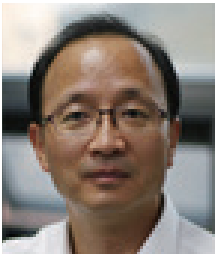
일자 2020년 11월 28일 (토) **장소** 온라인 컨퍼런스

접속 및 시청방법 등록자에 한하여 개별 공지

주최 한국정보보호학회 Korea Institute of Information Security & Cryptology **주관** 서울대학교 SEOUL NATIONAL UNIVERSITY

후원 국가정보원 National Intelligence Service Korea, 과학기술정보통신부, 행정안전부, KISA 한국인터넷진흥원, ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute, NSR 국가보안기술연구소, cen 아이티센 ITCEN

초대의 글



한국정보보호학회 회원 여러분, 안녕하십니까? 2020년도 한국정보보호학회 동계학술대회를 맞이하여 회원 여러분 모두의 안녕과 무궁한 발전을 기원합니다.

본 동계학술대회는 우리 학회에서 개최하는 주요 학술대회 중 하나로서, 1990년 학회 창립 이래 회원 여러분의 지대한 관심과 적극적인 참여에 힘입어 계속해서 발전해 오고 있는 대표적인 행사입니다. 특히 올해는 본 학회가 30주년을 맞이하게 된 뜻깊은 한 해이기도 합니다. 비록 COVID-19 확산이라는 초유의 사태를 겪고 있지만, 회원 여러분들의 연구에 대한 끊임없는 열정과 적극적인 참여에 힘입어 온라인 학술대회를 성공적으로 개최할 수 있게 되었습니다.

금년 동계학술대회는 서울대학교에서 개최되며, 온라인상에서 155편의 논문이 발표됩니다. 이 논문들은 정보보호의 초석인 암호를 비롯하여 시스템 보안, 네트워크 보안, 모바일 보안, IoT 보안, 디지털 포렌식, 정보보호 정책 및 제도, 그리고 최근 큰 관심을 받고 있는 인공지능보안, 블록체인 등 다양한 분야의 연구 결과를 망라하고 있습니다. 온라인 상에서 발표되는 논문들에 대한 실시간 채널을 개설하여, 연구자들 간의 활발한 소통이 이루어지는 행사가 되도록 기획하였습니다. 다양한 분야의 탁월한 연구 결과를 발표하시는 발표자들과 초청강연 연사이신 조현숙 전 소장님께 깊이 감사드리며, 이번 학술대회가 연구 결과 공유 및 소통을 위한 활발한 장이 되기를 기원합니다.

아울러 이번 대회를 위해 재정적으로 후원해 주신 회원사와 후원 및 협찬 기관들께 심심한 감사의 말씀 드립니다. 또한 어려운 여건 속에서도 성공적인 동계학술대회 준비를 위해서 수고해 주신 서울대 백윤흥 운영위원장과 연세대 권태경 프로그램 공동위원장, 인하대 이문규 프로그램 공동위원장을 비롯한 운영위원과 프로그램위원 여러분, 그리고 우리 학회 사무국 여러분께도 감사드리며, 행사가 성공적으로 마무리될 때까지 노력해 주시기를 부탁드립니다.

이번 학술대회가 온라인 학술대회의 우수 사례로 자리매김하고, COVID-19 사태의 어려움을 전화위복의 기회로 삼아 우리나라 정보보호 산업과 기술 경쟁력을 한 차원 더 발전시키는 계기가 되기를 기원합니다.

감사합니다.

2020. 11. 28

한국정보보호학회 회장 **정 수 환**

위원회

학술대회장 한국정보보호학회 회장 정수환 (숭실대학교)

조직위원회

- 조직위원장 이경현 (부경대학교)
- 조직위원 김익균 (한국전자통신연구원), 류재철 (충남대학교), 박상우 (국가보안기술연구소), 박영호 (세종사이버대학교), 원유재 (충남대학교), 유준상 (한국정보기술연구원), 이경호 (고려대학교), 이동범 (한국정보보산업협회), 이석래 (한국인터넷진흥원), 이옥연 (국민대학교), 임강빈 (순천향대학교), 차국헌 (서울대학교), 하재철 (호서대학교)

프로그램 위원회

- 프로그램위원장 권태경 (연세대학교), 이문규 (인하대학교)
- 프로그램위원 강민석 (KAIST), 강홍구 (한국인터넷진흥원), 곽진 (아주대학교), 김소정 (국가보안기술연구소), 김승주 (고려대학교), 김종성 (국민대학교), 김태성 (충북대학교), 김형식 (성균관대학교), 김형종 (서울여자대학교), 김호원 (부산대학교), 김휘강 (고려대학교), 김희석 (고려대학교), 도경화 (건국대학교), 문대성 (한국전자통신연구원), 박기웅 (세종대학교), 박종환 (상명대학교), 백유진 (우석대학교), 서승현 (한양대학교), 서정택 (순천향대학교), 서화정 (한성대학교), 손경호 (강원대학교), 손수엘 (KAIST), 손태식 (아주대학교), 신상욱 (부경대학교), 유일선 (순천향대학교), 윤명근 (국민대학교), 윤주범 (세종대학교), 윤지원 (고려대학교), 이광수 (세종대학교), 이덕규 (서원대학교), 이만희 (한남대학교), 이정현 (숭실대학교), 이종혁 (세종대학교), 이창훈 (서울과학기술대학교), 이태진 (호서대학교), 임을규 (한양대학교), 최대선 (숭실대학교), 최병철 (한국전자통신연구원), 허준범 (고려대학교)

운영위원회

- 운영위원장 백윤흥 (서울대학교)
- 운영위원 권동현 (부산대학교), 권태경 (서울대학교), 문현곤 (울산과학기술원), 윤종희 (영남대학교), 이병영 (서울대학교), 이상근 (고려대학교), 조영필 (한양대학교)

우수논문상

상장명	논문제목 / 저자 (소속)
과기정통부 최우수논문상	저성능 RISC-V 프로세서를 위한 고속 ARIA 암호 Extension 이진재, 김민재, 박종욱, 김호원 (부산대학교)
행정안전부 최우수논문상	디지털포렌식 관점에서의 암호키 재사용 취약점을 이용한 앱 데이터 복호화 연구 박진성, 서승희, 석병진, 이창훈 (서울과학기술대학교)
학회 최우수논문상	실행코드에서 미공개 S-box 획득 및 분석 : 삼성 스마트폰 펌웨어에 적용 김성겸, 김동훈 (고려대학교), 홍득조 (전북대학교), 성재 철(서울시립대학교), 홍석희 (고려대학교)
국가보안기술연구소 우수논문상	LTE 표준 프로토콜 기반 임시 식별자 매핑 공격 방지 기법 박철준, 배상욱, 이지호, 손민철, 김동관, 손수엘, 김용 대(KAIST)
	커버리지 기반 딥러닝 퍼징 기술의 유효성 검증 박래현, 김재욱, 정수창, 권태경 (연세대학교)
한국전자통신연구원 우수논문상	전이학습을 통한 적응형 모델 기반의 서버리스 On-Device 안드로이드 악성코드 탐지 기법 심현석, 정수환 (숭실대학교)
	ARIA에 대한 Shifting Retracing 부메랑 공격 백승준, 박종현, 김종성 (국민대학교)
한국인터넷진흥원 우수논문상	스켈레톤 정보를 이용한 저작권 침해 의심 영상 저작물 탐지 기법 김찬희, 유호제, 정아윤, 오수현 (호서대학교)
	모바일 TPM 및 가상화 기술을 활용한 신뢰 실행 환경의 보안성 향상 한승균, 장진수 (충남대학교)
학회 우수논문상	Android에서의 최신 블루투스 zero-click RCE 취약점 분석 부경욱, 이병영 (서울대학교)
	Adversarial Attacks to Neural Networks on Manufacturing Product Image Data 정병길, 이상근 (고려대학교)
	더미와 셔플링에 대한 효율적인 딥러닝 기반 프로파일링 부채널 분석 김주환, 한동국 (국민대학교)
	Samsung Pay Protocol Analysis and Safety 심승용, 윤원준, 박성진, 여종민, 유일 선(순천향대학교)
	NVIDIA CUDA PTX를 활용한 SIMECK 병렬 구현 장경배, 김현준, 임세진, 서화정 (한성대학교)
	탈중앙형 자기 주권 신원 데이터의 다자간 거래를 위한 안전한 비식별화 연구 조강우, 정병규, 신상욱 (부경대학교)
	커널 서브시스템 및 모듈 격리 기법에 대한 연구 유준승, 서지원, 방인영, 백윤흥 (서울대학교)

초청강연

• 초청강연 : 미래의 사이버보안

(조현숙 전 국가보안기술연구소 소장)

세션

세션	논문제목 / 저자 (소속)
블록체인 1	DID 학생증 서비스 모델 제안 강민정, 강지윤, 이지은, 조승현, 장설아, 이경현 (부경대학교)
	Private/Permissioned 블록체인에서의 데이터 프라이버시 및 익명화 기술 분석 김명길 (스마트엠투엠/부산대학교), 강솔 (스마트엠투엠)
	DApp 구현에서의 블록체인과 데이터베이스 데이터처리속도 비교 분석 강유림, 김지수, 김지원, 최나래, 김형종 (서울여자대학교)
	블록체인 기반 공정한 부인 방지 서비스에 관한 고찰 정병규, 조강우, 신상욱 (부경대학교)
	블록체인 기반 학생회비 전자장부 김명진, 정세윤, 김민정, 김경재, 강성원, 이경현 (부경대학교)
블록체인 2	A Review of Blockchain Interoperability and Its Current Solutions Muhammad Firdaus, Kyung-Hyune Rhee (Pukyong National University)
	블록체인 기반의 공공도서관 통합 이용자 관리시스템 장설아, 이경현 (부경대학교)
	허가형 블록체인 시스템의 합의 알고리즘의 보안성 및 성능 분석 이길희, 김형식 (성균관대학교)
	스마트 시티에서의 블록체인 기반 데이터 활용 방안 이민경, 곽진 (아주대학교)
	비콘 데이터 교환 및 블록체인 기반의 전염병 접촉자 구별 시스템 아키텍처 김건오, 김선균 (부경대학교)

세션

세션	논문제목 / 저자 (소속)
시스템 보안 1	DLL 인젝션과 API 후킹을 이용한 악성코드 분석에관한 연구 최용철, 이덕규 (서원대학교)
	Efficient Features for Matching Multi-Architecture Binary Executables Sami Ullah and Heekuck Oh (Hanyang University)
	유해한 데이터 경쟁 상태 탐지법 사례 조사 이광무, 이병영 (서울대학교)
	Binary Analysis Platform(BAP) 확장 구현 방법 유동민, 오희국 (한양대학교)
	한국인터넷진흥원 우수논문상 모바일 TPM 및 가상화 기술을 활용한 신뢰 실행 환경의 보안성 향상 한승균, 장진수 (충남대학교)
	Linux Kernel Data Structure Analysis for Data Flow Integrity 김주희 (서울대학교)
시스템 보안 2	군 무기체계 보호를 위한 안티탬퍼링 기술 동향 조명현, 황동일, 장지원, 남기빈, 백윤흥 (서울대학교)
	드론 마이크로 커널의 신뢰성을 위한 Control-flow Integrity 기반 Checkpoint/Restart 메커니즘에 대한 연구 조광수, 곽지원, 김승주 (고려대학교)
	RISC-V 기반 코어의 보안 인터페이스를 확장한 코드 재사용 탐지 기법 연구 황동일, 조명현, 장지원, 백윤흥 (서울대학교 전기정보공학부, 반도체공동연구소)
	임베디드 펌웨어 테스트 최신 기술 동향 정세연, 황은비, 조민기, 권태경 (연세대학교)
	학회 우수논문상 커널 서브시스템 및 모듈 격리 기법에 대한 연구 유준승, 서지원, 방인영, 백윤흥 (서울대학교)
	엔트로피와 TLSH를 이용한 미확인 펌웨어 이미지 식별 방법 김윤정, 김문선, 이만희 (한남대학교)
인공지능과 보안 1	적대적 예제와 전이학습 박희강, 최형기 (성균관대학교)
	AI 보안의 문제점과 한계 박수곤 (동명대학교), 이정훈 (인제대학교), 김동현 (영남대학교)
	인공지능을 활용한 악성코드 분류 기법 동향 조윤기, 안선우, 이영한, 전소희, 백윤흥 (서울대학교)
	앙상블 모델을 활용한 클라이언트 사이드 기반 웹 공격 대응에 관한 연구 김형민, 오수현, 임예린, 정현성, 홍지원, 조재현 (Best of the Best), 김경곤 (Naif Arab University for Security Sciences), 김현민 (금융보안원)
	기계학습 모델에 대한 적대적 공격 및 방어 기법 동향 심준석, 김호원 (부산대학교)

세션

세션	논문제목 / 저자 (소속)
인공지능과 보안 2	랜섬웨어 대비 자동 백업 리눅스 커널 모듈과 암호화 파일 탐지를 위한 Grayscale 이미지 분류 박건호, 김성보, 고상준, 유안지, 신동명 (엘에스웨어)
	딥러닝을 활용한 저작권 침해 의심 음원 탐지 기법 정아윤, 유호제, 김찬희, 오수현 (호서대학교)
	한국인터넷진흥원 우수논문상 스켈레톤 정보를 이용한 저작권 침해 의심 영상 저작물 탐지 기법 김찬희, 유호제, 정아윤, 오수현 (호서대학교)
	국가보안기술연구소 우수논문상 커버리지 기반 딥러닝 퍼징 기술의 유효성 검증 박래현, 김재욱, 정수창, 권태경 (연세대학교)
	특징 맵의 노이즈 제거를 통한 적대적 공격 방어 조현진, 김호원 (부산대학교)
인공지능과 보안 3	GAN을 이용한 이상탐지 시스템에 관한 연구 이영우, 조관용, 문현준, 윤주범 (세종대학교)
	특징 추출을 위한 CNN 기법 분석 및 LSTM 기반의 딥페이크 영상 탐지 연구 곽송이, 심현석, 정수환 (숭실대학교)
	보안 분야에서의 합성곱 신경망 기술 연구 동향 임세진, 강예준, 김현지, 장경배, 서화정 (한성대학교)
	Machine Learning Data Poisoning Quantification using Linear Discriminant Analysis Hyeongmin Cho, Sangkyun Lee (Korea University)
	Vulnerability of Federated Learning due to Malicious Dongjun Min, Sangkyun Lee (고려대학교)
인공지능과 보안 4	적대적 공격기법에 대한 차속 예측 1D CNN 모델의 취약성 권준형, 이상근 (고려대학교)
	API sequence를 이용한 AI 악성코드 탐지 비교 이윤호, 김주영, 신경아, 이상진 (고려대학교)
	모델 증류기법을 활용한 압축 CNN의 강건성 강화 이정현, 이상근 (고려대학교)
	적대적 예시 탐지를 위한 뉴런 기반 커버리지 기법의 적합성 연구 정수창, 박래현, 권태경 (연세대학교)

세션

세션	논문제목 / 저자 (소속)
디지털 포렌식	안드로이드 카카오톡 앱 삭제 시 SQLite 복구 연구 정다안, 손태식 (아주대학교)
	Ragnar Locker 랜섬웨어 데이터 복호화 방안 연구 강수진, 이세훈, 김소람, 김종성 (국민대학교)
	APFS 기반의 macOS 기기에서의 포렌식 기법 이진오, 손태식 (아주대학교)
	협업 툴의 사용자 행위별 아티팩트 분석 연구 – 윈도우즈 및 안드로이드 환경의 Microsoft Teams를 대상으로 김영훈, 권태경 (연세대학교)
	콘솔 게임기 아티팩트 분석 : 불법 콘텐츠 재생을 위한 익스플로잇 현황을 중심으로 김인영, 조민정, 이창훈 (서울과학기술대학교)
	행정안전부 최우수논문상 디지털포렌식 관점에서의 암호키 재사용 취약점을 이용한 앱 데이터 복호화 연구 박진성, 서승희, 석병진, 이창훈 (서울과학기술대학교)
클라우드 보안	Edge Computing의 특징 및 도전과제 분석 변원준, 임한울, 윤주범 (세종대학교)
	하이퍼바이저 취약점 분석 도구 개발 명철우, 이병영 (서울대학교)
	컨테이너의 호스트 자원 남용 관련 연구 동향 곽진한, 이병영 (서울대학교)
	Intel SGX와 부채널 공격 방어 기법에 대한 연구 장지원, 조명현, 김현준, 오현영, 백윤흥 (서을대학교)
	분산컴퓨팅 환경에서 효율적인 분산 트랜잭션 추적을 위한 샘플링 오버헤드 연구 이병용, 최상훈, 박기웅 (세종대학교)
네트워크 보안 1	다자간얽힘 스와핑을 통한 양자 패킷 스누핑에 대한 연구 박포일 (한국원자력통제기술원)
	TLS 1.2와 TLS 1.3의 성능 비교 및 분석 이상민, 맹주완, 이승훈, 유일선 (순천향대학교)
	5G 이동통신 보안기술 현황 김선엽, 김성겸 (고려대학교), 홍득조 (전북대학교), 성재철 (서울시립대학교), 홍석희 (고려대학교)
	Lattice 기반 양자 내성 키 교환 메커니즘과 전자 서명의 TLS 활용 가능성 분석 권희용, 최선호, 서민균, 이문규 (인하대학교)

세션

세션	논문제목 / 저자 (소속)
네트워크 보안 2	VPN 환경에서 SIEM을 활용한 공격 탐지 기법 연구 류호경 (고려대학교)
	A Study on Fault Detection in LTE Network: A Black-Box Testing for LTE Network Components Jiho Lee, Hongil Kim, Sangwook Bae, Mincheol Son, CheolJun Park, Seokbin Yun, Yeongbin Hwang, Yongdae Kim (KAIST)
	무선 공유기별 초기 패스워드 보안 수준 분석과 이에 따른 무선 공유기 패스워드 패턴 및 보안 수준 강화에 관한 연구 김종식, 조재현, 최예지, 염정현 (중부대학교)
금융 보안	다크웹 데이터를 이용한 비트코인 트랜잭션 클러스터링 기법 이진희, 김민재, 허준범 (고려대학교)
	익명화처리와 연합학습의 성능비교를 통한 효용성 분석 장진혁, 최대선 (숭실대학교)
	VASP 식별을 위한 가상자산 거래 특징 분석 연구 강홍구, 신용희, 박순태 (한국인터넷진흥원)
	중고 거래 사기 방지 플랫폼 제안 현장호, 이현호, 임다연, 이진우, 이창엽, 오동빈, 최원영 (Best of Best)
산업 보안	스마트공장 보안에 관한 연구 박재성 (고려대학교)
	STRIDE 위협 모델링을 이용한 스마트 팜 위협 분석 및 보안 요구사항 연구 강동석, 강민송, 김현수, 배진웅, 이충일, 조소현, 원요한, 홍현경, 지한별 (Best of Best), 김경곤 (Naif Arab University for Security Sciences)
	학회 우수논문상 Adversarial Attacks to Neural Networks on Manufacturing Product Image Data 정병길, 이상근 (고려대학교)
	발전소의 무선통신 보안위협과 보안 요구사항 및 보안조치 분석 정다운, 김창훈, 이주찬, 김준원, 최현표, 서정택 (순천향대학교)
	산업용 무선통신기술 보안 요구사항 개발을 위한 적용요건 연구 김장훈, 이주찬, 정다운, 서정택 (순천향대학교)

세션

세션	논문제목 / 저자 (소속)
인증 및 ID 관리 1	생체정보를 활용한 사용자 인증 프로토콜의 문제점 고찰 노승일 (광운대학교), 신영주 (고려대학교)
	보안과 편리성이 강화된 FIDO 인증 기반 무선 공유기 제어 시스템 개발 최가영, 이진아, 김지현, 박지현, 김형종 (서울여자대학교)
	FIDO2 프로토콜을 이용한 무인택배보관함 서비스 구현 진혜윤, 강민지, 염흥열 (순천향대학교)
	위임서명 기반의 모바일 자동차 키 공유 모델 김의진, 곽진 (아주대학교)
인증 및 ID 관리 2	DID에서의 공개키 알고리즘을 활용한 선택적 자격증명 제안 최중현, 조현우, 박은혜 (영산대학교), 정소연 (대진대학교),한승훈 (아주대학교), 안준연 (호서대학교)
	구독-발행 모델에 분산 식별자와 검증가능한 자격즉명 모델을 적용한 식별자 및 접근 관리 메커니즘 남혜민, 박창섭 (단국대학교)
	그룹서명을 이용한 전자출입명부 시스템 손우정, 박승민, 이은표, 오선식, 신명수, 이승준, 한종호, 윤기순, 전상현 (Best of the Best)
	DID 기반 신원 인증 시스템 이상현, 강원태, 김호원 (부산대학교)
해킹과 취약점 분석 1	리눅스 커널 익스플로잇 자동화 연구 동향 분석 이유찬, 이병영 (서울대학교)
	전자칠판 보안 취약점 분석 및 대응 방안에 관한 연구 박태호, 이주영, 지혜원, 김재준, 노시은, 박승원, 한철규, 양정규 (Best Of the Best)
	Stripped 바이너리 함수 심볼 예측방법 기술동향 김문회, 사미울라, 유동민, 이석원, 오희국 (한양대학교)
	Mach-O 바이너리를 지원하는 바이너리 분석 유틸리티 동향 조사 이석원, 오희국, 김문회, 유동민 (한양대학교)

세션

세션	논문제목 / 저자 (소속)
해킹과 취약점 분석 2	그리드 컴퓨팅 기반 실시간 스트리밍 서비스의 보안 위험성 탐구 김태호 (수원대학교), 윤태식, 윤승민 (고려대학교), 명수환 (연세대학교), 황선홍 (전남대학교), 이상진 (고려대학교)
	문서형 악성코드 분석 및 대응방안 연구 정준영, 이문규, 서정택 (순천향대학교)
	리눅스 커널 자원 경쟁 취약점 유형 분류 백민우 (고려대학교), 황준봉 (한양대학교), 조제진 (고려대학교)
	모의 공격을 통한 MAVLink 프로토콜 취약점 분석 한주홍, 위한샘, 이옥연 (국민대학교)
	빅데이터를 활용한 악성코드 탐지의 관한 연구 류경근, 이덕규, 최용철 (서원대학교)
개인정보보호	공공데이터 비식별화 기법 개선 방안 이재성, 김태성 (충북대학교)
	학회 우수논문상 탈중앙형 자기 주권 신원 데이터의 다자간 거래를 위한 안전한 비식별화 연구 조강우, 정병규, 신상욱 (부경대학교)
	의료 빅데이터에 대한 ε-차분 프라이버시 적용 임정묵, 김태성 (충북대학교)
	마이크로모빌리티 서비스의 QR코드 인증 취약점 분석 및 대응 방안 정해선, 곽진 (아주대학교)
암호이론과 구현 1	완전동형암호 라이브러리 분석: TFHE 이강훈, 윤지원 (고려대학교)
	Post-Quantum Secure Oblivious Transfer on Hard Homogeneous Spaces 김태찬, 김진수, 신준범 (삼성리서치)
	NIST 경량암호 공모사업 후보 알고리즘 HyENA의 안전성 분석 동향 김주헌, 김시은, 박종현, 백승준, 김종성 (국민대학교)
	NIST 경량암호 공모사업 후보 알고리즘 COMET의 안전성 분석 동향 김수빈, 김소은, 조세희, 백승준, 김종성 (국민대학교)
	한국전자통신연구원 우수논문상 ARIA에 대한 Shifting Retracing 부메랑 공격 백승준, 박종현, 김종성 (국민대학교)

세션

세션	논문제목 / 저자 (소속)
암호이론과 구현 2	오픈소스 기반 격자 방식 PQC 알고리즘 분석 김민하, 문학준, 우사이먼성일 (성균관대학교)
	프라이버시를 위한 영지식증명과 블록체인 기반의 익명인증 기법 및 개발 검증 연구 김태훈, 라경진, 이임영 (순천향대학교)
	SPN 암호의 불변 순열 공격 연구 정건상, 김성겸 (고려대학교), 홍득조 (전북대학교), 성재철 (서울시립대학교), 홍석희 (고려대학교)
	블록 암호 구조와 대수적 차수 관계 분석 김제성, 김성겸 (고려대학교), 홍득조 (전북대학교), 성재철 (서울시립대학교), 홍석희 (고려대학교)
	양자암호통신 국내외 기술 분석 이동섭, 류재철 (충남대학교)
IoT/CPS 보안 1	IoT 환경에서 무인증서 기반의 공개 검증 가능한 다중 수신자 Signcryption 방법에 관한 연구 이대휘, 이임영 (순천향대학교)
	IoT 환경에서 안전한 데이터 수집 저장을 위한 인증서 기반의 집계서명 기법에 관한 연구 황용운, 이임영 (순천향대학교)
	드론 기반 무선 센서 네트워크 최신 보안 프로토콜 분석 오상윤, 정재열, 정익래 (고려대학교), 변진욱 (평택대학교)
	DLMS/COSEM 프로토콜에서의 보안 설계 및 가용성 분석 오진혁, 이옥연 (국민대학교)
IoT/CPS 보안 2	IoT 기반 고위험 의료장치의 신뢰성 보장을 위한 홋수제어 기반 소자 설계 안성규, 주재경,최기철, 정혜림, 박기웅 (세종대학교)
	바디 센서 네트워크를 위한 Iqbal et al.의 키 교환 인증 기법 분석 및 정형화 검증 두구마 다니엘절비, 이상민, 김보남, 유일선 (순천향대학교)
	IoT 애플리케이션 대상 MITM 공격 취약점 분석 및 대응방안 진호준, 황영하, 서정택 (순천향대학교)
	OTP 시간동기화 인증을 활용한 IP카메라에 대한 연구 김대영, 이덕규 (서원대학교)

세션

세션	논문제목 / 저자 (소속)
정보보호 정책, 법, 제도	각국의 IoT 보안 인증제도의 분석을 통한 국내 IoT 보안 인증 제도의 개선안 김의현, 염흥열 (순천향대학교)
	EU-GDPR을 통한 국내 데이터3법 및 개인정보보호의 적절성 박유림, 신용태 (숭실대학교)
	텍스트 네트워크 분석을 활용한 국가 사이버안보 전략 분석: 미국과 영국 전략을 중심으로 송민경, 김동희, 김소정 (국가보안기술연구소)
	COVID-19 방역 프로세스 內 개인정보보호에 관한 연구 최진혁, 박동균, 김동영, 류재하, 박상수, 조현수, 이예은, 김영옥, 한철규 (Best of Best)
소프트웨어 보안	버퍼 오버플로우를 막기 위한 bounds-checking 연구동향 이영한, 서지원, 전소희, 조윤기, 백윤흥 (서울대학교)
	Dangling Pointer 방어에 대한 연구 방인영, 카욘도 마틴, 유준승, 서지원, 백윤흥 (서울대학교)
	학회 최우수논문상 실행코드에서 미공개 S-box 획득 및 분석: 삼성 스마트폰 펌웨어에 적용 김성겸, 김동훈 (고려대학교), 홍득조 (전북대학교), 성재철 (서울시립대학교), 홍석희 (고려대학교)
	커널 및 커널 드라이버의 격리된 환경에 대한 연구 서지원, 조윤기, 유준승, 백윤흥 (서울대학교)
	커널 어드레스 새니타이저 분석 안도현, 조민기, 진호용, 권태경 (연세대학교)
	정적 분석과 동적 분석을 이용한 취약함수 자동 식별 알고리즘 최여정, 양희동, 이만희 (한남대학교)
	임베디드 디바이스 펌웨어 퍼징 기술의 동향 분석 황은비, 정세연, 조민기, 권태경 (연세대학교)

세션

세션	논문제목 / 저자 (소속)
모바일 보안	**한국전자통신연구원 우수논문상** 전이학습을 통한 적응형 모델 기반의 서버리스 On-Device 안드로이드 악성코드 탐지 기법 심현석, 정수환 (숭실대학교)
	생체 정보와 MAC 주소를 결합 사용한 사용자 인증 및 접근 통제 솔루션 연구 김혜린, 안재윤, 장단비, 김명주 (서울여자대학교)
	국가보안기술연구소 우수논문상 LTE 표준 프로토콜 기반 임시 식별자 매핑 공격 방지 기법 박철준, 배상욱, 이지호, 손민철, 김동관, 손수엘, 김용대 (KAIST)
	학회 우수논문상 Android에서의 최신 블루투스 zero-click RCE 취약점 분석 부경욱, 이병영 (서울대학교)
	학회 우수논문상 삼성페이 프로토콜 분석 및 안전성 심승용, 윤원준, 박성진, 여종민, 유일선 (순천향대학교)
	6G를 향한 보안 기술 장찬국, 한주홍, 윤승환, 이옥연 (국민대학교)
	VoLTEFuzz: VoLTE 환경에서의 SIP 구현 취약점 탐지를 위한 분석 도구 개발 윤석빈, 배상욱, 손민철, 김동관, 이지호, 박철준, 황영빈, 김용대 (KAIST)
정보보호 표준, 평가, 인증	ISO/IEC 27701 분석을 통한 개인정보보호 관리체계 개선방안 제안 송어진, 유경아, 송인성, 고현희, 염홍열 (순천향대학교)
	정보시스템 위험평가를 위한 SUDA방법론 최다은, 조태희, 김태성 (충북대학교)
	UAS 보안인증 시험을 위한 보안 요구사항 이세윤, 장찬국, 이옥연 (국민대학교)
	클라우드 컴퓨팅 서비스 보안 인증제도 개선사항 김태완, 김현기, 장찬국, 이옥연 (국민대학교)
	CSfC 내 MSC 솔루션 보안요구사항 비교 분석 정서우, 오진혁, 장찬국, 이옥연 (국민대학교)

세션

세션	논문제목 / 저자 (소속)
부채널 분석 1	블록암호 SIMON 카운터 최적화 구현 분석 권혁동, 장경배, 김현지, 서화정 (한성대학교)
	NIST 경량암호 공모전 2라운드 후보 알고리즘 성능 분석 김현지, 권혁동, 장경배, 서화정 (한성대학교)
	딥러닝 기반의 부채널 분석 기술 연구 동향 심민주, 김현지, 박재훈, 서화정 (한성대학교)
	클라우드 환경에서 Intel 내장 GPU를 이용한 은닉 채널 공격 김태훈 (광운대학교), 신영주 (고려대학교)
	학회 우수논문상 NVIDIA CUDA PTX를 활용한 SIMECK 병렬 구현 장경배, 김현준, 임세진, 서화정 (한성대학교)
	과기정통부 최우수논문상 저성능 RISC-V 프로세서를 위한 고속 ARIA 암호 Extension 이진재, 김민재, 박종욱, 김호원 (부산대학교)
	개선된 리플-캐리 덧셈기 양자회로 (An Improvement of Quantum Ripple-Carry Addition Circuit) Harashta Tatimma Larasati, Janghyun Ji, Howon Kim (부산대학교)
부채널 분석 2	RISC-V ISA 암호 extension 연구 동향 분석 김민재, 박종욱, 김호원 (부산대학교)
	하드웨어 트로이잔 개요 및 분류 윤영여, 이진재, 김호원 (부산대학교)
	형태보존 암호 FEA에 대한 마스킹과 최적화기법의 제안 및 구현 김현준, 장경배, 서화정 (한성대학교)
	더미와 셔플링을 제거하는 신경망 설계 및 학습 방안 김주환, 문혜원, 심보연, 한동국 (국민대학교)
	학회 우수논문상 더미와 셔플링에 대한 효율적인 딥러닝 기반 프로파일링 부채널 분석 김주환, 한동국 (국민대학교)
	해밍웨이트 기반 이진 레이블을 사용한 비프로파일링 딥러닝 부채널 공격 배대현, 황종배, 이희경, 하재철 (호서대학교)

세션

세션	논문제목 / 저자 (소속)
부채널 분석 3	AVR 프로세서에서의 SEED 알고리즘 구현 박재훈, 권혁동, 장경배, 김현준, 서화정 (한성대학교)
	캐시 부채널 공격에 대응하는 T-Table 셔플링 기반 AES 구현 배대현, 황종배, 하재철 (호서대학교)
	RISC-V 환경에서 Curve25519의 Reduction 최적화 연구 김영범, 송진교, 서석충 (국민대학교)
	32-bit RISC-V에서의 LEA 최적화연구 곽유진, 김영범, 서석충 (국민대학교)
	NEON을 활용한 NIST 양자암호 SABER에서 다항식 곱셈 기반 Toom-Cook 알고리즘 최적화 연구 송진교, 김영범, 서석충 (국민대학교)
	OpenCL을 사용한 NIST LWC 2 라운드 후보 ESTATE 병렬연산 최적구현 박보선, 서석충 (국민대학교)
부채널 분석 4	GPU 환경에서의 SHA-3 최적화 구현 동향 최호진, 서석충 (국민대학교)
	중복데이터를 이용한 16비트-MSP430 환경에서의 HIGHT 알고리즘 오류공격 대응 연구 고의석, 박보선, 서석충 (국민대학교)
	GPU 환경에서의 효율적인 Number Theoretic Transform 최적화 구현 안상우, 서석충 (국민대학교)
	마스킹에 대한 신규 신경망 설계 방안 김주환, 한동국 (국민대학교)
	ARM Cortex-M4 환경에서 SIMD 명령어를 이용한 CHAM-64/128 최적화 연구 이정민, 송진교, 서석충 (국민대학교)
	행렬-벡터 곱에 대한 전력 부채널 분석 김규상, 박동준, 김희석, 홍석희 (고려대학교)

학술대회 등록방법

◉ 논문모집일정

- 논문제출 마감: 2020년 11월 4일 (수)
- 최종논문 제출 마감 2020년 11월 16일 (월)
- 논문발표자 사전등록 마감: 2020년 11월 16일 (월)
- 대회 일자: 2020년 11월 28일 (토)
- 심사결과 통보: 2020년 11월 11일 (수)
- 발표자료(동영상) 제출 마감: 2020년 11월 16일 (월)
- 일반참가자 사전등록 마감: 2020년 11월 25일 (수)

◉ 등록비 및 등록방법

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

*금번 학술대회는 현장등록이 없습니다.

- 학회 홈페이지(www.kiisc.or.kr)접속 ▶ 학회행사 ▶ 사전등록 바로가기 클릭 ▶ 2020 동계학술대회
- 사전등록 송금처: 예금주 한국정보보호학회
  계좌번호 (국민은행) 754-01-0008-146
- 사전등록 시 등록비는 위의 계좌로 송금하시고, 입금자가 대리일 경우 통보바랍니다.
- 신용카드 결제 시 계산서 발급이 불가합니다. (부가가치세법 시행령 제 57조)
- 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) 동계학술대회 등록 홍길동-"동홍길동" 기재
- 등록자의 핸드폰 번호로 모바일 상품권(학술대회 기념품)이 발송될 수 있으니, 반드시 본인 핸드폰 번호를 정확하게 기재하시어 불이익이 없으시길 바랍니다.
- 논문발표자 사전등록: 2020년 11월 16일(월)까지
  - 논문발표자의 경우, 사전 등록 시 논문번호 기재 - 각 논문 당 최소 1명의 저자는 등록해야 합니다.
    (미등록 시 논문게재목록에서 제외됩니다.)
- 일반참가자 사전등록: 2020년 11월 25일(수)까지

◉ 기타 안내 사항

※ 정회원(종신)을 제외한 학생가 등록은 학교 이외에 다른 소속이 없어야 합니다.
※ 회원가 등록은 학회 회원으로 가입을 하고, 1년 이내 연회비가 납부된 활동회원에 준합니다.
※ 신규회원 가입방법
학회 홈페이지 회원광장 ▶ 회원가입
입회비(신규 회원가입 시 납부): 5천원, 정회원 연회비: 5만원, 학생회원 연회비: 2만원 (신규회원 가입 시 입회비와 연회비 모두 납부가 되어야 합니다)

- 학회 특별회원사 임직원은 정회원가로 등록 가능합니다.
  - 학회 홈페이지(www.kiisc.or.kr) ▶ 회원광장 ▶ 특별회원사에서 확인하실 수 있습니다.
- 학생(대학원생)/학부생/고교생은 학회 메일로 학생증 사본 송부 부탁드립니다.
- 등록자에게는 논문전체가 수록된 온라인 프로시딩과 프로그램북, 모바일기념품이 제공됩니다.

학술대회 등록방법

- 등록확인서는 학회홈페이지 상단 '행사 등록확인서 바로가기'를 클릭하신 후, 등록 시 기재하신 성함과 이메일을 기재하시면 출력 가능합니다.
- 참가확인서는 kiisc@kiisc.or.kr 로 행사명, 성명, 소속을 기재하시어 행사 종료 후 요청하시기 바랍니다. (등록 시 기재하신 메일로 확인서 발송)

◉ 문의처

- (06132) 서울특별시 강남구 논현로 507 (역삼동 성치하이츠3차) 909호
- 행사문의: TEL: (02) 564-9333 (#2)
- 계산서 문의: TEL (02) 564-9333(#3)
- FAX: (02) 564-9226
- E-mail: kiisc@kiisc.or.kr

당신이 오늘 만날 수 있는 혁신

Innovation & Reality

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

2020 한국정보보호학회 동계학술대회

CISC-W'20

Conference on Information Security and Cryptography-Winter 2020

한국정보보호학회
Korea Institute of Information Security & Cryptology