한국정보보호학회
Korea Institute of Information Security & Cryptology

2019 한국정보보호학회 동계학술대회

CISC-W'19

Conference on Information Security and Cryptography-Winter 2019

일시 2019. 11. 30(토)

장소 중앙대학교(흑석동)

주최 한국정보보호학회 Korea Institute of Information Security & Cryptology

주관 중앙대학교 CHUNG-ANG UNIVERSITY

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

초대의 글

2019년도 한국정보보호학회 동계학술대회를 맞이하여 회원 여러분 모두의 무궁한 발전을 기원드립니다.

본 동계학술대회는 우리 학회에서 개최하는 주요 학술대회 중 하나로서 회원 여러분의 지대한 관심과 적극적인 참여에 힘입어 1990년 학회 창립 이래 계속해서 발전해 오고 있는 대표적인 행사입니다.

금년 동계학술대회는 중앙대학교에서 구두발표 세션 및 포스터발표 세션에서 약 160여편의 논문이 발표됩니다. 이 논문들은 정보보호의 초석인 암호이론 뿐만 아니라 IoT 보안, 시스템 보안, 부채널 분석을 비롯하여, 최근 큰 관심을 받고 있는 인공지능보안, 블록체인 등을 다루고 있어 다양한 보안 분야의 보안 연구자 및 실무자간 토론을 도모할 수 있는 자리가 될 것으로 기대합니다.

또한, 논문 발표와 더불어 최근 학계에 많은 관심을 얻고 있는 6개 분야(AI보안, 부채널분석, IoT보안, 차세대인증, CPS보안, 5G보안)를 선정하여 최신 기술에 관한 멀티 튜토리얼을 진행합니다. 이를 통해 해당 분야에 관심을 가진 많은 학생들과 교수님들, 그리고 각 분야 전문가가 특정 분야에 대한 최신 트렌드를 배우고 토론하는 유익한 시간이 될 것입니다. 더욱이, 이 튜토리얼들은 각 동일 주제의 연구회에서 주관함으로써 최근 활성화되고 있는 연구회와 본 학회의 학술대회가 동시 활성화되는 시너지효과가 발생되는 첫 학술대회가 될 것입니다.

특히, 본 동계학술대회는 주제 강연으로 우리나라 3대 정보보호 기관인 국가보안기술연구소, 한국인터넷진흥원, 한국전자통신연구원의 보직자를 모시고 각 연구기관의 소개와 인재 채용 동향을 듣는 시간을 준비했습니다. 이 3개 기관은 우리나라의 정보보호 기술 및 정책을 연구, 개발, 운영하는 대표적 기관으로써 정보보호를 전공하는 대부분의 학생들이 일하고 싶어하는 직장입니다. 학생들을 지도하는 교수님들 또한 제자들의 진로 지도를 위해 많은 도움이 되리라 믿습니다.

마지막으로 이번 동계학술대회 준비를 위해서 많은 수고를 해주신 운영위원회 및 프로그램위원회 위원님들과 학회관계자, 그리고 후원기관 관계자 분들께 감사의 말씀을 드립니다.

2019. 11. 30

한국정보보호학회 회장 **이 경 현**

조직도

학술대회장 이경현(한국정보보호학회 학회장)

조직위원회

- 조직위원장 홍만표(아주대학교)
- 조직위원 정수환(숭실대학교), 류재철(충남대학교), 하재철(호서대학교), 이옥연(국민대학교), 임강빈(순천향대학교), 박영호(세종사이버대학교), 이경호(고려대학교), 김정덕(중앙대학교), 박상우(국가보안기술연구소), 유준상(한국정보기술연구원), 이민수(한국정보보호산업협회)

운영위원회

- 운영위원장 최명길(중앙대학교), 이정현(숭실대학교)
- 운영위원 강정민(국가보안기술연구소), 김동찬(국민대학교), 김상춘(강원대학교), 김태성(충북대학교), 김찬문(한국수자원공사), 안준호(교통대학교), 염용진(국민대학교), 윤영태(국가보안기술연구소), 이용필(한국인터넷진흥원), 장영우(인천국제공항공사), 최민하(EY한영), 최희봉(국가보안기술연구소)

프로그램 위원회

- 프로그램위원장 이만희(한남대학교)
- 프로그램위원 곽 진(아주대학교), 김종성(국민대학교), 김형식(성균관대학교), 김호원(부산대학교), 김휘강(고려대학교), 김희석(고려대학교), 도경화(건국대학교), 박기웅(세종대학교), 백유진(우석대학교), 서정택(순천향대학교), 서화정(한성대학교), 손수엘(KAIST), 신인철(목포대학교), 유일선(순천향대학교), 윤명근(국민대학교), 윤종희(영남대학교), 윤주범(세종대학교), 윤지원(고려대학교), 이덕규(서원대학교), 이병영(서울대학교), 이종혁(상명대학교), 이창훈(서울과기술대학교), 정익래(고려대학교), 최대선(공주대학교), 최윤호(부산대학교), 최은정(서울여자대학교), 한동국(국민대학교), 홍득조(전북대학교)

프로그램일정표

시간	트랙 A 310관 611호	트랙 B 310관 612호	트랙 C 310관 701호	트랙 D 310관 702호	트랙 E 310관 703호	트랙 F 310관 704호	포스터트랙 P 310관 로비
08:00 ~ 09:00	등록						
09:00 ~ 10:00	A1 자동차보안	B1 IoT보안	C1 AI보안	D1 부채널분석	E1 네트워크보안	F1 사이버정책	P1 블록체인 보안/ 해킹 및 취약점 분석
10:00 ~ 10:10	휴식						
10:10 ~ 11:10	A2 해킹 및 취약점분석	B2 모바일보안	C2 AI보안	D2 부채널분석	E2 시스템보안	F2 블록체인보안	P2 암호이론/ 평가/인증/ 교육
11:10 ~ 11:20	휴식						
11:20 ~ 12:20	A3 해킹 및 취약점분석	B3 차세대인증	C3 암호이론	D3 부채널분석	E3 시스템보안	F3 블록체인보안	P3 IoT 보안/ 모바일 보안/ 네트워크 보안/ AI 보안
12:20 ~ 13:10	중식(310관 지하4층 학생식당)						
13:10 ~ 14:10	A4 콘텐츠 보안	B4 CPS보안	C4 암호이론	D4 포렌식	E4 HW보안	F4 금융보안	P4 시스템보안/ 은닉채널
14:10 ~ 14:20	휴식						
14:20 ~ 15:20	차세대인증 튜토리얼	CPS보안 튜토리얼	AI보안 튜토리얼	부채널분석 튜토리얼	5G보안 튜토리얼	IoT 보안 튜토리얼	
15:20 ~ 15:30	휴식						
15:30 ~ 16:30	**초청강연(310관 505호)** 좌장: 운영위원장 이정현 숭실대학교 3대 정보보호 기관(ETRI, KISA, NSR) 소개 및 인재 채용 동향 ETRI 김익균 본부장, KISA 심원태 본부장, NSR 손기욱 본부장						
16:30 ~ 17:00	**개 회 식(310관 505호)** 개 회 사: 학회장 이경현 부경대학교 학회관련안내: 운영위원장 최명길 중앙대학교 우수논문 시상 및 경품추첨						
17:00 ~ 17:10	휴식						
17:10 ~ 18:00	**정기총회(310관 904호)**						

우수논문상

시상내역	논문 제목
행안부장관상	음악 스트리밍 프로파일링 기반의 불법 음악 스트리밍 사이트 탐지 방안 정해선, 곽진(아주대)
과기부장관상	블록체인 노드의 네트워크 고립을 방지하는 전파 프로토콜 제안 김미연(NSHC), 염흥열(순천향대)
학회장최우수상	딥러닝 기술을 활용한 S-box 구조 식별 방법 김동훈, 김성겸(고려대), 홍득조(전북대), 성재철(서울시립대), 홍석희(고려대)
ETIR 원장상	표준 웹 기능을 활용한 디바이스 핑거프린팅 기반 사용자 식별 모델 박소희, 최대선(공주대)
ETIR 원장상	Hardware Performance Counter를 이용한 Meltdown 공격 프로세스 동적 탐지 방법 김문선, 박승수, 이만희(한남대)
KISA 원장상	새로운 인증 패러다임 오라(ORA: one round authentication) - 보안 USB를 활용한 단말 대 단말 1 라운드 인증 프로토콜 설계 및 구현 강병민(평택대),안홍규(평택대, 인젠트), 변진욱(평택대)
KISA 원장상	모바일 포렌식 도구를 통한 효과적인 iPhone 내 디지털 증거 수집 절차에 대한 연구 안재혁, 손태식(아주대)
NSR 소장상	키워드 검색 기반의 이미지 증거 분석 유동민, 오희국(한양대)
NSR 소장상	스마트 그리드 환경에서 안전한 통신을 위한 사용자 인증 및 키 합의 방식의 보안 취약점 분석 및 대응방안 박기성, 노성기, 윤대근(ETRI)
학회장 우수상	UI 은닉 기반의 안드로이드 Inter-Procedural Control Flow Graph 난독화 기법 심현석, 윤홍선, 정수환(숭실대)
학회장 우수상	STRIDE 위협 모델링 기법을 이용한 Digital Signage 플랫폼 취약점 분석 및 대응방안 홍현경, 신현욱, 고준영, 권동현, 소찬영, 김지섭, 심기욱, 한철규(BoB)
학회장 우수상	Permissioned Blockchain에서의 Privacy를 위한 OKSA기반 익명인증 기법에 관한 연구 라경진, 이임영(순천향대)
학회장 우수상	서버리스 플랫폼에서의 정확한 요금 산정을 위한 초 저지연 리소스 미터링 모듈 최상훈, 이병용, 박건호, 박기웅(세종대)
학회장 우수상	비선형 불변 공격에 저항성을 갖는 최적의 비트 순열에 관한 연구 정건상, 김성겸(고려대), 홍득조(전북대), 성재철(서울시립대), 홍석희(고려대)
학회장 우수상	차분 딥러닝 분석 성능 향상을 위한 새로운 구조 제안 권동근, 진성현, 김한빛, 홍석희, 김희석(고려대)
학회장 우수상	하드웨어 암호IP 테스트를 위한 SoC보드상에서의 AMBA AXI환경 구축 이진재, 지장현,박종욱, 김호원(부산대)
학회장 우수상	국내 이통사 USIM 인증 알고리즘 부채널분석 취약성 이태호, 한동국(국민대)

구두발표 트랙 A

310관 611호

발표 세션	발표논문
A1 자동차 보안 09:00 ~ 10:00 좌장 장남수(세종사이버대)	자동차 소프트웨어 보안 개발 프로세스를 위한 요구사항 정승연, 강수영, 김승주(고려대)
	스마트 자동차 전자제어장치(ECU)의 보안취약점 분석 및 해결방안 마련 이기옥, 장남수(세종사이버대)
	V2X 환경에서의 차량 내 인증서 관리시스템 보안성 평가항목 연구 김태경, 지청민,김지민, 홍만표(아주대)
	V2V 통신 안전성 평가를 위한 DoS 공격 연구 동향 이승영, 지청민, 김지민, 홍만표(아주대)

발표 세션	발표논문
A2 해킹 및 취약점 분석 10:10 ~ 11:10 좌장 노건태(서울사이버대)	STRIDE 위협 모델링 기법을 이용한 Digital Signage 플랫폼 취약점 분석 및 대응방안 홍현경, 신현욱, 고준영, 권동현, 소찬영, 김지섭, 심기욱, 한철규(BOB)
	Syma X8 드론에 대한 취약점 분석 김예준, 강수영, 김승주(고려대)
	DDR4 메모리의 보안 취약점을 통한 보안 위협 검증 강지훈, 류재철(충남대)
	코드 인젝션을 통한 데이터 탈취 가능성 연구 김찬진, 염흥열(순천향대)

발표 세션	발표논문
A3 해킹3 11:20 ~ 12:20 좌장 장항배(중앙대)	Key-value쌍 입력을 통한 CGI Fuzzing 정재영, 조성준, 김창현(한양대)
	RAW 이미지 뷰어 취약점 분석 황선홍, 이병천(중부대)
	최신식의 화이트 박스 퍼징 도구에 대한 성능 비교 평가 김주환, 이성호, 최세호, 윤주범(세종대)
	커버리지 기반 퍼징 최신 기술 분석 정세연, 정수창, 김서영, 조민기, 권태경(연세대)

구두발표 트랙 A

발표 세션	발표논문
A4 **콘텐츠 보안** 13:10 ~ 14:10 좌장 곽 진(아주대)	음악 스트리밍 프로파일링 기반의 불법 음악 스트리밍 사이트 탐지 방안 정해선, 곽진(아주대)
	공공 인프라 영상보안을 위한 보안 프레임워크 연구 유진용, 김영갑(세종대)
	클라우드 공유 기능의 저작권 침해 방지를 위한 연구 박소희, 곽진(아주대)
	공공장소 CCTV 프라이버시 확보 기법 권혁동, 장경배, 권용빈, 서화정(한성대)

튜토리얼	발표논문
차세대인증 14:20 ~ 15:20 좌장 최대선(공주대)	DID 개념과 영지식 증명 황정연 박사(ETRI)

구두발표 트랙 B

310관 612호

발표 세션	발표논문
B1 IoT보안 09:00 ~ 10:00 좌장 임을규(한양대)	Efficient Lightweight Authentication Scheme for Internet of Things Application Abhijeet Thakare, 이의종, 김영갑(세종대)
	임베디드 OS에서의 메모리 보호 메커니즘 적용 한계성 권순홍, 이종혁(상명대)
	IoT 플랫폼 상호운용을 위한 OCF 게이트웨이 구현 Naufal Suryanto, Ismail, Harashta Tatimma Larasati, 허신욱, 김호원(부산대)
	IoT 기기 보안 기술 검증을 위한 사물 봇 공격 자동화 도구 연구 황송이(UST), 김정녀(ETRI)

발표 세션	발표논문
B2 모바일보안 10:10 ~ 11:10 좌장 이정현(숭실대)	모바일 포렌식 도구를 통한 효과적인 iPhone 내 디지털 증거 수집 절차에 대한 연구 안재혁, 손태식(아주대)
	UI 은닉 기반의 안드로이드 Inter-Procedural Control Flow Graph 난독화 기법 심현석, 윤홍선, 정수환(숭실대)
	Android 어플리케이션에서 사용된 Third-party Library 탐지 기술 동향 분석 이석원, 이연준, 오희국(한양대)
	안드로이드 어플리케이션 레벨에서 호출 가능한 보안 컨테이너 환경 구현 기법 윤재현, Ngoc-Tu Chau, Hoang Nguyen Huy, 정수환(숭실대)

발표 세션	발표논문
B3 차세대인증 11:20 ~ 12:20 좌장 도경화(건국대)	새로운 인증 패러다임 오라(ORA: one round authentication) - 보안 USB를 활용한 단말 대 단말 1 라운드 인증 프로토콜 설계 및 구현 강병민(평택대),안홍규(평택대, 인젠트), 변진욱(평택대)
	표준 웹 기능을 활용한 디바이스 핑거프린팅 기반 사용자 식별 모델 박소희, 최대선(공주대)
	Permissioned Blockchain에서의 Privacy를 위한 OKSA기반 익명인증 기법에 관한 연구 라경진, 이임영(순천향대)
	최소행위 중 EEG 기반 사용자인증 연구 남승수, 최대선(공주대)

구두발표 트랙 B

발표 세션	발표논문
B4 CPS보안 13:10 ~ 14:10 좌장 윤주범(세종대)	스마트 그리드 환경에서 안전한 통신을 위한 사용자 인증 및 키 합의 방식의 보안 취약점 분석 및 대응방안 박기성, 노성기, 윤대근(ETRI)
	Concepts on Improving Nuclear Control Inspection through Augmented Reality 박포일(한국원자력통제기술원)
	국내 전력 시스템에서의 SSL VPN 가용성 분석 오진혁, 이옥연(국민대)
	내부자 위협에 의한 정보유출 방지를 위한 기술적, 관리적 보안대책에 관한 연구 변예은(한국원자력통제기술원)

튜토리얼	발표논문
CPS보안 14:20 ~ 15:20 좌장 서정택(순천향대)	제어시스템 운영환경에서의 이상행위 탐지기술 김형천 실장(NSR)

구두발표 트랙 C

310관 701호

발표 세션	발표논문
C1 AI보안 09:00 ~ 10:00 좌장 이옥연(국민대)	딥러닝 기술을 활용한 S-box 구조 식별 방법 김동훈, 김성겸(고려대), 홍득조(전북대), 성재철(서울시립대), 홍석희(고려대)
	언어 규칙 기반 DGA-DNS 머신러닝 분류 모델링 이동주(순천향대), 강성묵(강남대)
	진화-생산적 적대 신경망에 기반한 악성 소프트웨어 탐지 장용남, 원동욱, 이성환(고려대)
	디지털 점 분장을 통한 딥러닝 기반 얼굴인식 모델 기만공격 류권상, 최대선(공주대)

발표 세션	발표논문
C2 AI보안 10:10 ~ 11:10 좌장 손수엘(KAIST)	위협 인텔리전스를 이용한 위협 경보와의 연관분석 및 결과구축 방법론 이종진, 배근우, 한인성, 조성영(국방과학연구소)
	음성 인식 시스템에 대한 공격과 방어 김예은, 이연준, 오희국(한양대)
	CNN과 바이트 평균을 활용한 데이터 조각 파일타입 분류에 관한 연구 조현수, 김견우, 김재현, 원종은, 윤현호, 조재현, 김재희(BOB), 김영옥(현대자동차), 한철규(LG CNS)
	LSTM Neural Network를 기반으로 한 전자문서 보안등급 산정 기준 수립에 관한 연구 김정욱, 송성욱, 장항배(중앙대)

발표 세션	발표논문
C3 암호이론 11:20 ~ 12:20 좌장 김종성(국민대)	NIST 2라운드 Ring LWE 기반 공개키 암호 기법 동향 분석 박소현, 이동훈(고려대)
	NIST 경량 암호 공모사업 2라운드 후보에 대한 구조 분석 백승준, 김영범, 전용진, 김종성(국민대)
	RLWE 기반 분산형 그룹키 교환 방식의 성능 분석 한성호, 최락용, 김광조(카이스트)
	NIST 경량암호 공모사업 1라운드 탈락 AEAD에 대한 안전성 분석 송진교, 이종혁, 박보선, 전용진, 김종성(국민대)

구두발표 트랙 C

발표 세션	발표논문
C4 암호이론 13:10 ~ 14:10 좌장 김광조(KAIST)	비선형 불변 공격에 저항성을 갖는 최적의 비트 순열에 관한 연구 정건상, 김성겸(고려대학교), 홍득조(전북대학교), 성재철(서울시립대학교), 홍석희(고려대학교)
	LWE 기반 퍼지 추출기 연구 동향 임일환, 이동훈(고려대)
	최신 경량 블록 암호 동향 이종혁, 김원일, 한정민, 전용진, 김종성(국민대)
	Lattice의 Determinant를 활용한 효율적인 GNFS 다항식 선택기법 전찬호, 김수리(고려대), 윤기순(NSHC), 장남수, 박영호(세종사이버대), 김창한(세명대), 홍석희(고려대)

튜토리얼	발표논문
AI보안 14:20 ~ 15:20 좌장 조영필(숭실대)	인공지능 기반 보안 문제 이재구 교수(국민대)

구두발표 트랙 D

310관 702호

발표 세션	발표논문
D1 부채널분석 09:00 ~ 10:00 좌장 서석충(국민대)	NIST Round2 양자내성암호 공모전 코드기반암호 성능 비교 분석 최승주, 장경배, 김현지, 서화정(한성대)
	Fixed-Base Comb 스칼라 곱 알고리즘에 대한 단일파형 부채널 공격 향상 기법 박동준, 이상엽, 조성민, 김희석, 홍석희(고려대)
	mbedTLS 상에서의 양자내성암호 적용 가능성 연구 윤영여, 박찬희, 손수민(부산대), 이지은(한국인터넷진흥원), 김호원(부산대)
	비트 퍼뮤테이션 기반 블록 암호에 대한 신규 부채널 분석 동향 임성혁, 문혜원, 박소연, 우지은, 이태호, 한동국(국민대)
	Rowhammer 취약점을 이용한 공격 분석 양희동, 이만희(한남대)
	안드로이드 스마트폰 전자파 오류 주입 공격 자동화 시스템 제안 이종혁, 임한섭, 한동국(국민대)

발표 세션	발표논문
D2 부채널분석 10:10 ~ 11:10 좌장 서화정(한성대)	GPU 병렬 환경에서의 AES 암호 최적화 연구 안상우, 서석충(국민대)
	소수 특성을 활용한 RLWE 최적화 구현 이주엽, 김수리, 홍석희(고려대)
	ARIA 암호 알고리즘 TVLA 통계 검증 기법 제안 박한별, 김주환, 심보연, 서석충(국민대), 장상윤(NSR), 한동국(국민대)
	동적 분석 기반 공개키 암호알고리즘의 부채널 취약 구현 평가 연구 이예찬(고려대), 박태환(NSR), 진성현, 김한빛, 김희석(고려대)
	가상화 환경에서 메모리 중복제거 기능을 이용한 KASLR 공격 김태현, 김태훈, 신영주(광운대)
	주파수 기반 스마트폰 카메라 동작 탐지 전자파 분석 연구 이지우, 한동국(국민대)

구두발표 트랙 D

발표 세션	발표논문
D3 **부채널분석** 11:20 ~ 12:20 좌장 김희석(고려대)	CPU 환경에서 PBKDF2-HMAC-SHA256 최적화 연구 최호진, 서석충(국민대)
	Hardware Performance Counter를 이용한 Meltdown 공격 프로세스 동적 탐지 방법 김문선, 박승수, 이만희(한남대)
	그림 파형을 이용한 비프로파일링 기반 딥러닝 공격 원유승(난양기술대), 박종연(삼성전자), 한동국(국민대)
	블록 암호에 대한 부채널 분석용 전력 파형 데이터 셋 구축 배대현, 하재철(호서대), 강유성, 김태성, 최두호(ETRI)
	비트슬라이스 구현 블록암호에 대한 향상된 부채널 분석 기법 – Case Study : Robin 김연재, 김수진, 한재승, 한동국(국민대)
	FPGA 부채널분석 시험 보드를 활용한 8비트 MCU 기반 소프트웨어 부채널분석 플랫폼 구현 강준기, 이봉수(NSR)
	차분 딥러닝 분석 성능 향상을 위한 새로운 구조 제안 권동근, 진성현, 김한빛, 홍석희, 김희석(고려대)
	국내 이통사 USIM 인증 알고리즘 부채널분석 취약성 이태호, 한동국(국민대)

발표 세션	발표논문
D4 **포렌식** 13:10 ~ 14:10 좌장 임강빈(순천향대)	키워드 검색 기반의 이미지 증거 분석 유동민, 오희국(한양대)
	디지털 포렌식을 위한 Android 및 Windows 환경에서 카카오톡 아티팩트 분석(II) 이나비, 김광조(KAIST)
	드롭박스 포렌식 데이터 획득 기법 김은진, 황현욱, 손기욱(NSR)
	윈도우 아티팩트 생성 추적 방안 고신우(서울여자대), 이건우(고려대), 이세영(경북대), 이충호(한세사이버보안고), 정희태(조선대)

튜토리얼	발표논문
부채널분석 14:20 ~ 15:20 좌장 하재철(호서대)	SW 암호 실행의 메모리분석을 이용한 부채널분석 박태환 박사(NSR)

구두발표 트랙 E

310관 703호

발표 세션	발표논문
E1 네트워크보안 09:00 ~ 10:00 좌장 신인철(목포대)	WBAN 환경에서의 안전한 1라운드 인증 프로토콜 최재현, 오상윤, 탁금지, 정익래(고려대), 변진욱(평택대)
	FANET 환경에서의 효율적인 Proxy Signature 기법 오상윤, 정익래(고려대)
	소프트웨어 정의 네트워크(SDN)를 대상으로 한 퍼즈테스팅의 평가 위성일, 김현태, 이현주, 손수엘(KAIST)
	Newhope의 키 조정 메커니즘을 통한 Apon 등의 프로토콜 구체적 사례 검증 홍동연, 최락용, 김광조(KAIST)

발표 세션	발표논문
E2 시스템보안 10:10 ~ 11:10 좌장 신동훈(DGIST)	랜덤 메모리 할당을 이용한 향상된 스택 메모리 보호 기법 진홍주, 박문찬, 이동훈(고려대)
	커널 소프트웨어에 대한 방어 기법 연구 동향 채수민, 진홍주, 이동훈(고려대)
	Chrome Extension을 활용한 로그인 평문전송 탐지 및 차단 툴 개발 강동혁, 최영근, 박수진, 이장우, 손영락(BoB)
	자체 수정 코드 및 분석 기술 동향 류승호, 오희국(한양대)

발표 세션	발표논문
E3 시스템보안 11:20 ~ 12:20 좌장 안효범(공주대)	서버리스 플랫폼에서의 정확한 요금 산정을 위한 초 저지연 리소스 미터링 모듈 최상훈, 이병용, 박건호, 박기웅(세종대)
	Intel Processor Trace를 활용한 가상머신 수행 흐름 무결성에 관한 연구 서지원, 방인영, 백윤흥(서울대)
	Binary Diffing: An Empirical Analysis and Enhancements Sami Ullah, 오희국(한양대)
	가상 환경에서의 효과적인 트레이스 추출 방안에 대한 연구 방인영, 서지원, 백윤흥(서울대)

구두발표 트랙 E

발표 세션	발표논문
E4 HW보안 13:10 ~ 14:10 좌장 이병영(서울대)	하드웨어 암호IP 테스트를 위한 SoC보드상에서의 AMBA AXI환경 구축 이진재, 지장현, 박종욱, 김호원(부산대)
	TEE 기반의 Intel SGX 취약점 연구 동향 김경호, 권용빈, 김현지, 김현준, 서화정(한성대)
	공인인증서 유출 방지를 위한 Intel SGX 기반 관리 방안 연구 배재건, 공성현, 이창훈(서울과학기술대)
	Intel SGX에서의 Spectre 공격 분석 한찬희, 이만희(한남대)

튜토리얼	발표논문
5G보안 14:20 ~ 15:20 좌장 유일선(순천향대)	5G 엣지 보안 기술 박종근 책임(ETRI)

구두발표 트랙 F

310관 704호

발표 세션	발표논문
F1 사이버정책 09:00 ~ 10:00 좌장 이용석(국방부)	정보시스템 구축.보안지침 대한 47개 비교분석 류호경, 명성식, 이호준(고려대)
	ICT 공급망 보안관리 통제 개발을 위한 국내외 관련 기준 비교분석 고영현, 김정덕(중앙대)
	IT 공급망 해킹 동향 분석 김광준, 손효현, 이만희(한남대)
	화이트해커와 기업 분석을 통한 국내 버그바운티 활성화 방안 제시 하희헌, 정현경, 강민주, 지용빈, 이광진, 신예준(BOB)

발표 세션	발표논문
F2 블록체인보안 10:10 ~ 11:10 좌장 이창훈(서울과기대)	블록체인 노드의 네트워크 고립을 방지하는 전파 프로토콜 제안 김미연(NSHC), 염흥열(순천향대)
	블록체인에 특화된 개인정보영향평가 방안에 관한 연구 – 국내 개인정보보호법 및 허가형 블록체인을 중심으로 – 김경하, 장남수(세종사이버대)
	zk-SNARKs기반 블록체인 익명 인증 아키텍처 강원태, 김유나, 김호원(부산대)
	Permissioned 블록체인 환경에서의 안전한 키 생성에 대한 연구 김태훈, 이임영(순천향대)

발표 세션	발표논문
F3 블록체인보안 11:20 ~ 12:20 좌장 정익래(고려대)	블록체인 DID 동향 및 분석 이상현, 김용수, 김호원(부산대)
	로컬 원데이 메시지 블록체인을 활용한 차량 평판 시스템 설계 이수진, 서승현(한양대)
	블록체인 기반 DO-ABE를 이용한 커넥티드 카 데이터 공유 기법 정병규, 김혜빈, 신상욱(부경대)
	블록체인을 활용한 종량제 봉투 실명제 제안 심민주, 권용빈, 엄시우, 윤재웅, 임현빈, 서화정(한성대)

구두발표 트랙 F

발표 세션	발표논문
F4 **금융보안** 13:10 ~ 14:10 좌장 이병천(중부대)	안전한 전자상거래를 위한 보안 기법 연구: 온라인 현금자산 보안을 중심으로 박용현(KAIST), 조민주(동국대), 김남형(순천향대), 정재영(한양대), 이경민(동국대), 이준범(대구가톨릭대), 김홍진(LG CNS)
	QR코드와 추가인증서를 이용하는 간편결제 웹서비스 윤정민, 박종훈, 권혁민, 마민기, 이병천(중부대)
	Understanding Nine Central Bank Digital Currency Experiments Selected from the World Edwin Ayisi Opare, 김광조(KAIST)
	블록체인 네트워크 기반의 암호화폐 동향 분석 임세진, 김현지, 서화정(한성대)

튜토리얼	발표논문
IoT 보안 14:20 ~ 15:20 좌장 이덕규(서원대)	사물인터넷 보호를 위한 기기 인증 및 네트워크 보안 기술 임재덕 박사(ETRI)
	IoT 주요 보안 위협 및 대응방안 김대완 선임(KISA)

포스터 트랙 P

310관 로비

발표 세션	번호	발표논문
P1 **블록체인 보안/해킹 및 취약점 분석** 09:00 ~ 10:00 좌장 김기범(NSR)	1	블록체인을 활용한 관광 분석 시스템 제안 장경배, 최승주, 권혁동, 김경호, 서화정(한성대)
	2	블록체인을 이용한 호스트기반 악성코드 침입탐지 관제시스템에 관한 연구 최용철, 이덕규(서원대)
	3	블록체인 기반 릴라제로 분산 학습 기법 박승윤, 오희국(한양대)
	4	블록체인과 연합학습에 관한 연구 산디 라마디카, 이경현(부경대)
	5	매직키 획득을 위한 펌웨어 분석 임한울, 김현욱, 윤주범(세종대)
	6	라즈베리 파이를 활용한 스마트 스피커 및 NAS 로그 분석 신수민, 박세준, 강수진, 조승기, 이예솔, 김기윤, 김종성(국민대)
	7	디지털 복합기 RAW 9100 포트의 위험성 연구 김준태, 박소영, 윤지인, 윤형준, 이용우(BoB), 지한별, 박의성(라온화이트햇), 김홍진(LG CNS)
	8	임베디드 시스템 펌웨어 취약점 퍼저 분석 김현욱, 이규원, 김원철, 윤주범(세종대)
	9	윈도우 운영체제 환경에서의 파일리스 공격 기법 조사 이경호, 김기범(NSR)
	10	국내 APT 및 기업 보안 사고에 대한 고찰 이창엽(창원경일고), 이진우(대구대), 이정훈(인제대), 노무승(창원중앙고), 박현상(무안 남악중)
	11	네트워크 퍼저를 이용한 FTP 서버의 취약점 분석 최인호, 윤정준, 윤주범(세종대)
	12	차량 위협 모델과 보안 정책 고동의(안동 경일고), 박상우(대구 달성고)

포스터 트랙 P

발표 세션	번호	발표논문
P2 암호이론/ 평가/인증/ 교육 10:10 ~ 11:10 좌장 이덕규(서원대)	1	White-Box Cryptography의 사용 동향과 취약점에 관한 조사 연구 박예찬(한양대)
	2	암호 키관리 상호운용 프로토콜(KMIP)과 암호 키관리 솔루션(KMS) 동향 조사 김도원, 최은영, 박해룡(KISA)
	3	안전한 바이오인증을 위한 함수 암호 구현 연구 동향 전성윤, 임종혁, 이문규(인하대)
	4	해시 기반 서명 기법을 이용한 티켓 기반 서비스 제공 방법 지청민, 김지민, 홍만표(아주대)
	5	공동소유 환경을 제공하는 새로운 ID 기반 프록시 재암호화 김원빈, 이임영(순천향대)
	6	OSINT 기반 사이버 위협정보 수집 및 관리기술 연구 김민석, 강지훈(디플랫폼)
	7	학생회비의 투명성 제고를 위한 PBFT 합의 기반의 회계 감사 시스템 아키텍처 김건오, 김민혁, 김선균, 이소연, 노시완, 이경현(부경대)
	8	OSINT 개념과 활용방안 연구(Study on OSINT Concept and Use Cases) 유정훈, 고승철(수원대)
	9	커넥티드 의료기기 트래픽 분석 기반 사이버보안 자산 관리 연구 이준석(전남대), 정일안, 정동섭(휴네시온)
	10	영국 사례를 통해 본 한국 규제 샌드박스 시행의 현황 및 시사점 김지혜(KISCA), 염흥열(순천향대)
	11	정보보안 사고 사례 분석을 통한 정보보호 평가 항목 제안 주영국(고려대)
	12	기초 오펜시브 시큐리티 기법 실습을 위한 파이썬 기반 교보재 개발 이해영, 김태형, 임윤수, 박도규, 최승용(청주대)
	13	개인인증을 위한 심전도 데이터 취급 간 준용해야 할 유의사항 및 관련 지침 김경훈, 김동영, 김준서, 박예찬, 박인현, 오명교, 이우진, 이현정, 최재진(BoB)

포스터 트랙 P

310관 로비

발표 세션	번호	발표논문
P3 IoT 보안/ 모바일 보안/ 네트워크 보안/ AI 보안 11:20 ~ 12:20 좌장 윤종희(영남대)	1	기업환경에서 초기 IoT 보안 도입을 위한 지침 조한섭(고려대)
	2	In-body OTP : 이식형 의료 장치의 고유성 확보를 위한 체내형 One Time Password 생성 방법 안성규, 정혜림, 박기웅(세종대)
	3	IoT 환경을 위한 무인증서 기반의 게이트웨이 중재 서명 방법에 관한 연구 이대휘, 이임영(순천향대)
	4	종단 간 보안을 지원하는 MQTT-SN 보안 아키텍쳐 설계 및 구현 남혜민, 박창섭(단국대)
	5	스마트폰 환경의 보안부팅 기술 비교 분석 이정국, 김진우, 이상길(충남대), 이상한(NSR), 이철훈(충남대)
	6	안드로이드에서 JNI를 사용하는 공유라이브러리 동적분석에 대한 연구 최정수(고려대)
	7	LibFuzzer를 이용한 APK 클래스 모듈 분석 박기현, 이성원, 황신운, 윤종희(영남대)
	8	행위 기반의 지속인증을 위한 스마트폰 인증 연구 동향 분석 황은비, 박래현, 권태경(연세대)
	9	P2P 네트워크 기반 악성코드 분석 생태계 구현 방법 최지헌(아주대)
	10	임베디드 시스템의 RDP와 ARP 취약점 분석 및 해결방안 정이원, 허태겸(대구대 정보보호영재교육원)
	11	허니팟을 활용한 캠퍼스 네트워크 공격 유형 분석 오인영, 정지호(서원대), 김정태(ETRI), 강구홍(서원대)
	12	시스코 IOS FunctionTrace 알고리즘에 관한 연구 조현우, 이소연, 이예은, 안건희, 박성진, 박광호, 김경곤, 신정훈(BoB)
	13	머신러닝 프라이버시에 관한 연구 : FEDERATED LEARNING 아피파툴 무카로, 푸트리 라마와티, 김호원(부산대)
	14	머신러닝을 활용한 피싱사이트 탐지 방안 김경석, 김태호, 박우인(수원대)

포스터 트랙 P

발표 세션	번호	발표논문
P4 시스템보안/ 은닉채널 13:10 ~ 14:10 좌장 백유진(우석대)	1	위협 모델링을 통한 POS 시스템 보안 요구 사항 분석 김민수, 김대웅, 박건호, 박신철, 이승재, 임지훈(BoB), 이상섭(삼성리서치)
	2	PDF 악성 코드 탐지 방법과 발전에 관한 연구 이영한, 김요한, 하회리, 백윤흥(서울대)
	3	대량 악성코드 자동화 분석 프레임워크 이성원, 전현규, 박기현, 윤종희(영남대)
	4	Windows 10 Timeline을 이용한 사용자 행위 분석 현주연, 김재희, 김가은, 김성욱, 김하늘, 송찬영(BoB), 김영철(삼일회계법인), 허원석(BoB)
	5	SNI 차단 및 암호화 연구 윤재웅, 김경호, 서화정(한성대)
	6	리눅스 오픈소스 바이너리 프로텍터 분석 문현준, 송준환, 윤주범(세종대)
	7	시스템 호출 데이터를 활용한 비정상 행위 탐지 연구 김요한, 하회리, 김현준, 백윤흥(서울대)
	8	Multi-Variant Execution Environment를 위한 데이터 난수화 기법 김현준, 황동일, 김지환, 백윤흥(서울대)
	9	효율적인 Multi-Variant Execution Environment에 대한 연구 장지원, 김지환, 황동일, 신장섭, 백윤흥(서울대)
	10	Power Delivery Chip 기반의 은닉 채널 정혜림, 안성규, 박기웅(세종대)
	11	음향 신호를 이용한 은닉채널 동향 연구 이선우, 이동훈(고려대)
	12	USBEE의 은닉 채널을 활용한 데이터 유출 방지를 위한 주파수 탐지 기술 제안 황태윤, 김서현, 한혜경, 윤지원(고려대)

※ 온라인 프로시딩 다운로드 안내

www.cisc.or.kr 상단 프로시딩 다운로드 탭에서 온라인 프로시딩 (전체논문수록) 다운로드

- 다운로드 비밀번호 : 2022
- 다운로드 기간 : 2019년 11월 30일(토)

학술대회 등록방법

◉ 논문모집일정

- 논문제출 마감 : 2019년 11월 13일(수)
- 심사결과 통보 : 2019월 11월 15일(금)
- 최종본 제출 : 2019년 11월 18일(월)
- 논문발표자 사전등록 마감 : 2019년 11월 20일(수)
- 일반참가자 사전등록 마감 : 2019년 11월 22일(금)

◉ 등록안내

	사전등록		현장등록
	회원	비회원	
정회원(종신)	100,000원	155,000원	170,000원
학생회원(대학원생)	80,000원	105,000원	120,000원
학부생/고교생	50,000원	50,000원	50,000원

※ 정회원(종신)을 제외한 학생가 등록은 학교 이외에 다른 소속이 없어야 합니다.
※ 회원가 등록은 학회 회원으로 가입을 하고, 1년 이내 연회비가 납부된 활동회원에 준합니다.
※ 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.
- 등록확인서는 행사 당일 제공해 드리는 명찰 안에 포함되어 있습니다.
- 등록자에게는 논문전체가 수록된 온라인 프로시딩과 프로그램북, 중식권1매가 제공됩니다.
(행사당일 www.cisc.or.kr에서 다운로드 가능, 비밀번호: 2022)

◉ 사전등록

- 학회 홈페이지(www.kiisc.or.kr)접속 ▶ 학술행사 ▶ 사전등록 바로가기 클릭 ▶ 2019 동계학술대회
- 사전등록 송금처: 예금주 한국정보보호학회
계좌번호 (국민은행) 754-01-0008-146
- 등록비는 필히 등록자명으로 입금해 주시기 바라며, 등록자와 입금자명이 다를 경우 학회로 통보하여 주셔야 입금확인이 가능합니다.
- 논문발표자 사전등록: 2019년 11월 20일(수)까지
  - 논문발표자의 경우, 사전 등록 시 논문번호 기재
  - 각 논문 당 최소 1명의 저자는 등록해야 합니다.(미등록 시 논문게재목록에서 제외됩니다.)
- 일반참가자 사전등록: 2019년 11월 22일(금)까지

◉ 문의처

- (06132) 서울특별시 강남구 논현로 507(역삼동 성지하이츠3차) 909호
- TEL: (02) 564-9333 (#1)
- FAX: (02) 564-9226
- E-mail: kiisc@kiisc.or.kr

행사장 안내

310관(100주년기념관)

101관(영신관) | 102관(약학대학 및 R&D센터) | 103관(파이퍼홀) | 104관(수림과학관)

105관(제1의학관) | 106관(제2의학관) | 107관(학생회관) | 201관(본관) | 202관(전산정보관)

203관(서라벌홀) | 204관(중앙도서관) | 207관(뵵스트홀) | 208관(제2공학관) | 209관(창업보육관)

301관(중앙문화예술관) | 302관(대학원) | 303관(법학관) | 304관(미디어공연영상관)

구 분	장 소(100주년 기념관(310관))
개회식(우수논문시상)	505호(5F)
정기총회	904호(9F)
구두발표	611호 ~ 612호(6F) / 701호 ~ 704호(7F)
포스터발표	로비(1F)
등록대	407호(4F)
등록자 중식	학생식당(지하4F)

행사장 안내

◉ 일반버스

지선버스	5511(서울대 → 중앙대), 5517(서울대 → 중앙대), 5524(신림8동 → 중대입구), 5529(삼막사 사거리 → 중앙대), 6411(구로동 → 개포동)
B간선버스	151(우이동 → 중앙대), 360(송파 → 여의도), 361(고덕동 → 영등포), 362(오금동 → 여의도), 363(송파 → 여의도), 640(신월동 → 삼성역), 642(방화동 → 고속터미널), 452(송파 → 중앙대병원)
R광역버스	9408(분당 → 영등포)
T마을버스동작	01(달마사 → 수산시장), 동작10(신동아아파트 → 절고개)
A공항버스	600(잠실 → 인천공항)

◉ 지하철

9호선	흑석역(중앙대입구역) : 3, 4번 출구에서 도보 15분
7호선	상도역(중앙대앞) : 5번 출구에서 도보 10분
4호선	동작역(또는 1호선 노량진역) 하차 후 흑석동 방향으로 걸어나와서 버스타고 10분거리 신용산역 3번출구 하차 후 151번 승차 → 중앙대병원 앞 하차
1호선	노량진역 1번 출구 마을버스 1번승차 → 중앙대병원 앞 하차 또는 학교셔틀버스 이용

기념품/경품안내

◉ 기념품 안내

[HABBSI] 고속무선충전 마우스패드

◉ 경품 안내

iPad 10.2형 128GB
1개

AirPods Pro
2개

삼성외장SSD T5 1TB
3개

NUGU candle
3개

스타벅스 상품권 1만원권
10개

*경품은 일부 변경될 수 있습니다.

MEMO

2019 한국정보보호학회 동계학술대회

CISC-W'19

Conference on Information Security and Cryptography-Winter 2019

한국정보보호학회
Korea Institute of Information Security & Cryptology