한국정보보호학회
Korea Institute of Information Security & Cryptology

한국정보보호학회 동계학술대회

CISC-W'18

Conference on Information Security and Cryptography-Winter 2018

일자 2018년 12월 8일(토) **장소** 세종대학교(군자관, 충무관)

주최 한국정보보호학회 Korea Institute of Information Security & Cryptology 주관 세종대학교 SEJONG UNIVERSITY

후원 국가정보원 National Intelligence Service Korea, 행정안전부, KISA 한국인터넷진흥원, ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute, NSR 국가보안기술연구소, LIG 넥스원, 보안프로젝트 www.hackerschool.org, kakao

초대의 글

2018년도 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 세종대학교에서 구두발표 세션 및 포스터발표 세션에서 약 160여편의 논문이 발표됩니다. 또한, 한국인터넷진흥원 주관의 정보보호 R&D 데이터 챌린지 세션이 진행됩니다.

본 동계학술대회에서 발표될 논문들은 정보보호의 초석이라 할 수 있는 제반 암호이론 뿐만 아니라 IoT 보안, 시스템 보안 등 다양한 응용환경에서 요구되는 정보보호기술, 그리고 관련 정책 및 표준들이 포함되어 있습니다. 이와 더불어 최근 이슈가 되고 있는 블록체인 세션 등을 마련하여 연구 결과에 대한 실무자간 토론 및 친목을 도모할 수 있는 자리를 마련하였습니다.

정보보호 분야는 몇 년 전부터 국가의 새로운 성장 동력으로 다양한 분야들과 융합을 하면서 점점 활동 영역을 넓혀가고 있는 가운데, 그 중요성과 위상이 더욱 높아지고 있습니다.

본 동계학술대회는 ICT 방송통신 융합과 정보보호를 주제로 학계, 산업계, 연구기관의 연구자뿐만 아니라, 정보보호 관련 정부기관, 민간기관 소속 전문가들 간의 학문적 교류 및 관련 연구를 수행하는 과정에서 도출된 새로운 연구결과를 발표하는 장이 될 것입니다.

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

2018. 12.

한국정보보호학회 회장 **홍 만 표**

조직도

• **학술대회장** 한국정보보호학회 회장 홍만표 (아주대학교)

• **조직위원회**

조직위원장	이동훈 (고려대학교)	
조직위원	공성곤 (세종대학교)	이경현 (부경대학교)
	김인중 (사이버안전훈련센터)	이옥연 (국민대학교)
	김정삼 (영남이공대학교)	정수환 (숭실대학교)
	류재철 (충남대학교)	하재철 (호서대학교)
	유준상 (한국정보기술연구원)	

• **운영위원회**

운영위원장	김영갑 (세종대학교)	
운영위원	강지원 (세종대학교)	박원형 (극동대학교)
	김남기 (경기대학교)	송재승 (세종대학교)
	김형종 (서울여자대학교)	신지선 (세종대학교)
	김호원 (부산대학교)	이광수 (세종대학교)
	문창주 (건국대학교)	이희조 (고려대학교)
	박규동 (국방과학연구소)	조규형 (한국정보기술연구원)
	박기웅 (세종대학교)	조상현 (네이버)
	박대섭 (세종대학교)	홍득조 (전북대학교)
	박래호 (한국전자통신연구원)	홍석희 (고려대학교)

• **프로그램위원회**

프로그램위원장	손태식 (아주대학교)	
프로그램위원	권태경 (연세대학교)	유일선 (순천향대학교)
	곽 진 (아주대학교)	이경호 (고려대학교)
	김기형 (아주대학교)	이문규 (인하대학교)
	김용대 (KAIST)	이정현 (숭실대학교)
	김종성 (국민대학교)	이창훈 (서울과학기술대학교)
	김형식 (성균관대학교)	임강빈 (순천향대학교)
	김휘강 (고려대학교)	임을규 (한양대학교)
	노승민 (성결대학교)	윤주범 (세종대학교)
	박영호 (세종사이버대학교)	여상수 (목원대학교)
	서정택 (순천향대학교)	장항배 (중앙대학교)
	예홍진 (아주대학교)	한동국 (국민대학교)
	안효범 (공주대학교)	양대헌 (인하대학교)

프로그램 일정표

시 간	트랙 A (202A)	트랙 B (208)	트랙 C (202)	트랙 D (209A)	트랙 E (210)	트랙 F (211)
08:00 –09:00	등 록 (충무관 209호)					
09:00 –10:00	A1 암호이론(Ⅰ)	B1 암호응용(Ⅰ)	C1 블록체인(Ⅰ)	D1 차량 보안	E1 포스터(Ⅰ)	F1 포스터(Ⅰ)
10:00 –10:20	휴 식					
10:20 –11:20	A2 암호이론(Ⅱ)	B2 암호응용(Ⅱ)	C2 블록체인(Ⅱ)	D2 디지털 포렌식	E2 포스터(Ⅱ)	F2 포스터(Ⅱ)
11:20 –11:30	휴 식					
11:30 –12:10	초청강연(암호 부채널 분석 동향, 한국전자통신연구원 최두호 박사) (군자관 6층 소강당 607호)					
12:10 –12:40	개회식 I (군자관 6층 소강당 607호) 개 회 사 : 학 회 장 홍만표 아주대학교 축 사 : 부 총 장 엄종화 세종대학교 학회관련안내 : 운영위원장 김영갑 세종대학교 우수논문 시상 및 경품추첨					
12:40 –13:40	중 식 (학생회관 1층)					
13:40 –14:40	A3 어플리케이션 보안	B3 해킹 및 취약점(Ⅰ)	C3 블록체인(Ⅲ)	D3 IoT 보안 (Ⅰ)	E3 부채널연구회 (Ⅰ)	DATA CHALLENGE
14:40 –14:50	휴 식					
14:50 –15:50	A4 인증 시스템	B4 해킹 및 취약점(Ⅱ)	C4 딥 러닝	D4 IoT 보안 (Ⅱ)	E4 부채널연구회 (Ⅱ)	DATA CHALLENGE
15:50 –16:00	휴 식					
16:00 –17:00	A5 악성코드	B5 보안성 평가 및 정책	C5 무선통신 보안	D5 5G 보안 연구회	E5 부채널연구회 (Ⅲ)	DATA CHALLENGE
17:00 –17:10	휴 식					
17:10 –18:00	정기총회 (군자관 6층 소강당 607호)					

우수논문 리스트

no.	시상내역	제출자소속	논문저자	논문제목
1	행안부장관상	한국과학기술원	최지원, 차상길	효율적 바이너리 코드 재조립 시스템의 설계
2	KISA원장상	고려대학교 전북대학교 서울시립대학교	조은지, 김성겸 박연지, 이용성 홍득조, 성재철 홍석희	CUDA를 활용한 차분 확률의 통계적 분석
3	KISA원장상	아주대학교	조윤기, 김지민 지청민, 홍만표	An effective way to identify similar functions by performing pre-processing for binary analysis
4	ETRI원장상	세종대학교, 국방과학연구소	박진호, 김도연 김두희, 윤현수 김용현, 김동화 신동규, 신동일	사이버전 피해평가 시뮬레이션 도구의 설계 및 구현
5	ETRI원장상	순천향대학교	김광훈, 염흥렬	ARP 스푸핑을 방지하기 위한 블록체인 활용 모델 제안
6	NSR소장상	한국뉴욕주립대학교 성균관대학교	우지혜, 전소윤 최지원, 김형식 우사이먼	사용자의 공인인증서에 관한 인식과 브라우저 선택에 미치는 영향 연구
7	NSR소장상	순천향대학교	박현성, 서정택	국내 암호화폐 거래소 보안위협 및 대응방안 제시
8	정보보호학회 최우수논문상	호서대학교	권홍필, 배대현 하재철	부채널 분석 공격에 대응하는 초경량 블록 암호 CHAM 구현을 위한 축소 마스킹 기법 적용
9	우수 논문상	연세대학교, 한국인터넷진흥원	오상진, 박래현 박준형, 권태경	악성코드 패밀리명의 Ground-Truth를 위한 레이블링 기법 연구
10	우수 논문상	한양대학교	임수민, 임을규	프로세스 가상 메모리 데이터 유사성을 이용한 메모리 주입 판단 방법
11	우수 논문상	한국과학기술원	이은규, 김용대	LTE 무선 접속 과정 취약점에 관한 연구
12	우수 논문상	고려대학교	이재웅, 석재혁 이동훈	딥러닝을 이용한 자동 취약점 분석
13	우수 논문상	국민대학교	김기윤, 신수민 이종혁, 김종성	말랑말랑 톡카페 애플리케이션 데이터베이스 복호화 방안 연구
14	우수 논문상	한국정보기술연구원 한성대학교	임지환, 조기윤 성민석, 정영호 김성범, 김경곤 이경문, 서화정	Z-Wave 보안 취약점 분석
15	우수 논문상	국민대학교	박한별, 심보연 문재근, 한동국	선형 연산 특성을 이용한 전력 분석 최적화 방안
16	우수 논문상	서울과학기술대학교	조민정, 이창훈	블록체인 기반의 산업제어시스템 접근 권한 관리
17	우수 논문상	한국정보기술연구원 차세대 보안리더 양성 프로그램, 드림에이스, 티오리	고영건, 문성훈 김재희, 조대환 오병윤, 유재욱 이 원, 신정훈	Mifare Classic 태그 타입 사용 출입 통제 시스템의 보안 취약점 및 대응방안에 대한 연구

구두발표 트랙 A

TRACK A – 충무관 202A호	
세션	**발표논문**
A1 암호이론(Ⅰ) 09:00 – 10:00 좌장 : 이광수 (세종대)	CUDA를 활용한 차분 확률의 통계적 분석 조은지, 김성겸, 박연지 (고려대학교), 홍득조 (전북대학교), 성재철 (서울시립대), 홍석희 (고려대학교)
	MILP를 활용한 차분 공격 및 선형 공격 관점에서의 PRINCE 블록 암호 분석 전용진, 이종혁, 박석원, 윤형준, 최예림, 김경란, 박태진, 조은영, 김종성 (국민대학교)
	확률 계산 방법에 따른 자동화 탐색의 효율성 분석 이상협, 김성겸, 이용성 (고려대학교), 홍득조 (전북대학교), 성재철 (서울시립대), 홍석희 (고려대학교)
	Linux환경에서 SP800-90B 엔트로피 분석도구의 효율적인 호출 방안 연구 이태호, 김현기, 송행권, 이옥연 (국민대학교)
A2 암호이론(Ⅱ) 10:20 – 11:20 좌장 : 한동국 (국민대)	완전동형암호화를 사용한 암호화된 데이터베이스 시스템 김태윤, 김형식 (성균관대학교)
	Homomorphic encryption 라이브러리를 이용한 암호화 바이너리의 String signature 탐색 구현 황태윤, 윤지원 (고려대학교)
	완전동형암호를 이용한 덧셈 연산: TFHE 소개와 구현 홍미연, 윤지원 (고려대학교)
	동형 암호를 이용한 효율적인 프라이버시 보존 헬스케어 시스템 박상우, 송주석 (연세대학교)
A3 어플리케이션 보안 13:40 – 14:40 좌장 : 이병천 (중부대)	말랑말랑 톡카페 애플리케이션 데이터베이스 복호화 방안 연구 김기윤, 신수민, 이종혁, 김종성 (국민대학교)
	모바일 환경에서의 광고 어플리케이션의 보안 취약점 분석 지우중, 김형식 (성균관대학교)
	안드로이드 앱 보호를 위한 동적 보호 기법 안티 에뮬레이션 분석 및 성능 평가 김문회, 오희국 (한양대학교)
	안드로이드 어플리케이션의 OAT 파일 무결성 검증 김수린, 최주섭, 김형식 (성균관대학교)

구두발표 트랙 A

A4 인증 시스템 14:50 - 15:50 좌장 : 박영호 (세종사이버대)	사용자의 공인인증서에 관한 인식과 브라우저 선택에 미치는 영향 연구 우지혜, 전소윤, 최지원 (한국뉴욕주립대학교), 김형식 (성균관대학교), 우사이먼 (한국뉴욕주립대학교)
	Mifare Classic 태그 타입 사용 출입 통제 시스템의 보안 취약점 및 대응방안에 대한 연구 고영건, 문성훈, 김재희, 조대환, 오병윤, 유재욱 (KITRI BoB), 이원 (드림에이스), 신정훈 (티오리)
	FIDO 기반의 웹 표준 인증을 위한 웹 브라우저 안전 저장소 시스템 설계 및 구현 박재연, 신동일, 신동규 (세종대학교), 이재영, 이형석 (㈜아이리플)
	함수암호를 이용한 차세대 인증 Template 보호 기술 박동희, 박영호 (세종사이버대학교)

A5 악성코드 16:00 - 17:00 좌장 : 양대헌 (인하대)	악성코드 패밀리명의 Ground-Truth를 위한 레이블링 기법 연구 오상진, 박래현 (연세대학교), 박준형 (한국인터넷진흥원), 권태경 (연세대학교)
	Firm-Pot: 악성코드 분석을 위한 대규모 펌웨어 허니팟 김민근, 김은수, 김동관, 김용대 (KAIST)
	API 별 가중치 기반 스코어링 기법을 적용한 파일 리스 악성코드 탐지 기법 연구 양정은 (서울여자대학교), 배순규 (중앙대학교), 오세준 (선린인터넷고등학교), 이세영 (미림여자정보과학고등학교), 최찬우 (서울디지텍고등학교), 김재성(동아대학교), 김기홍 (㈜세인트시큐리티), 전상현 (시큐레터㈜)

구두발표 트랙 B

TRACK B – 충무관 208호	
세션	**발표논문**
B1 암호응용(Ⅰ) 09:00 – 10:00 좌장 : 노건태 (서울사이버대)	스마트 컨트랙트의 취약한 의사난수 생성 분석 및 대응방안 이진경 (서울여자대학교), 김경민 (고려대학교), 정윤서 (한국디지털미디어고등학교), 이진우 (선린인터넷고등학교), 강연호 (거제제일고등학교), 김규헌 (고려대학교), 이상섭 (삼성리서치), 김경곤 (고려향대학교)
	블록체인 기반 인증 체계 구축 및 위협 분석 이가영, 이연수, 이혜지, 염흥렬 (순천향대학교)
	5G 환경을 위한 블록체인 기반 분산형 이동성 관리 기술 김이진, 최형기 (성균관대학교)
B2 암호응용(Ⅱ) 10:20 – 11:20 좌장 : 장항배 (중앙대)	효율적 바이너리 코드 재조립 시스템의 설계 최지원, 차상길 (KAIST)
	An effective way to identify similar functions by performing pre-processing for binary analysis 조윤기, 김지민, 지청민, 홍만표 (아주대학교)
	핸들러 기능 매핑을 사용한 VMProtect 가상화 코드내의 비교 연산자와 조건문 분석 전하람 (서울과학기술대학교)
	정적 바이너리 계측을 활용한 메모리 취약점 탐지기술 연구 김형석 (국가보안기술연구소), 김현태, 이승엽, 차상길 (KAIST)
B3 해킹 및 취약점(Ⅰ) 13:40 – 14:40 좌장 : 권태경 (연세대)	네이버 음성 CAPTCHA의 취약점 Case Study 분석 전소윤, 우지혜, 최지원 (한국뉴욕주립대학교), 김형식 (성균관대학교), 우사이먼 (한국뉴욕주립대학교)
	Return Oriented Programming 공격에 대한 방어 기법 동향 분석 장혜린, 박문찬, 진홍주, 이동훈 (고려대학교)
	macOS 커널에서의 보호기법과 우회방법 분석 이유찬, 권태경 (연세대학교)
	소프트웨어 취약점을 이용한 자동 exploit 생성 모듈 분석 이상무, 김주환, 윤주범 (세종대학교)

구두발표 트랙 B

B4 해킹 및 취약점(II) 14:50 – 15:50 좌장 : 윤주범 (세종대)	프로세스 가상 메모리 데이터 유사성을 이용한 메모리 주입 판단 방법 임수민, 임을규 (한양대학교)
	Data Space Randomization을 활용한 MVEE의 Variant 생성 기법 연구 황동일, 신장섭, 전성일, 백윤흥 (서울대학교)
	SSL 암호화 전 패킷 추출 연구 방안 김영수 (세종대학교), 원혜린 (서울여자대학교), 정재우, 류민수 (세종대학교), 김현지 (인하대학교), 김의연 (서울여자대학교), 김경곤 (고려대학교)
	Non-ActiveX 기반 금융보안모듈 취약점분석 이정민, 이주선, 이진우, 이준오, 이시훈, 박주현 (세종대학교)

B5 보안성 평가 및 정책 16:00 – 17:00 좌장 : 김범수 (연세대)	사이버전 피해평가 시뮬레이션 도구의 설계 및 구현 박진호, 김도연, 김두회, 윤현수 (세종대학교), 김용현, 김동화 (국방과학연구소), 신동규, 신동일 (세종대학교)
	임베디드 리눅스 시스템의 보안 설정 검사 방법 연구 김서영, 권태경 (연세대학교)
	국내 핀테크 정책 현황 김미연, 염흥열 (순천향대학교)
	미국 원자력시설의 사이버보안 규제 지침과 최신 개정안 비교 이재창 (한국원자력통제기술원)

구두발표 트랙 C

TRACK C – 충무관 202호	
세션	**발표논문**
C1 블록체인(Ⅰ) 09:00 – 10:00 좌장 : 박기웅 (세종대)	Solidity 기반 스마트 컨트랙트 시스템 퍼징을 위한 자동 코드 생성 기법 연구 김윤태, 이종협 (가천대학교)
	IoT 블록체인을 이용한 토큰 기반 권한 관리 박환, 김미선, 서재현 (목포대학교)
	ARP 스푸핑을 방지하기 위한 블록체인 활용 모델 제안 김광훈, 염흥열 (순천향대학교)
C2 블록체인(Ⅱ) 10:20 – 11:20 좌장 : 김기형 (아주대)	블록체인 기반의 산업제어시스템 접근 권한 관리 조민정, 이창훈 (서울과학기술대학교)
	국내 암호화폐 거래소 보안위협 및 대응방안 제시 박현성, 서정택 (순천향대학교)
	블록체인을 이용한 전자투표 장단점 분석 홍지형, 권희원, 김윤정 (서울여자대학교)
	블록체인 기반 차량데이터 관리 시스템 박승윤, 오희국 (한양대학교)
C3 블록체인(Ⅲ) 13:40 – 14:40 좌장 : 김종성 (국민대)	블록체인 소프트웨어의 취약점을 이용한 인젝션 공격에 대한 연구 김병국, 허준범 (고려대학교)
	EOS 암호화폐의 블록 생성에 대한 인센티브 분석 한성호, 안형철, 김광조 (KAIST)
	블록체인 기반 사용자 계정 관리 기술 동향 조사 이대화, 김베드로, 지우중, 김형식 (성균관대학교), 우사이먼 (한국뉴욕주립대학교)
	블록체인 기반의 소셜 미디어 플랫폼 분석을 통한 교내 탈중앙화 소셜 미디어 보상체계 제안 김범진, 김은수, 조수빈, 이지수, 김진우, 반주형, 이경모, 노시완, 이경현 (부경대학교)

구두발표 트랙 C

C4 딥 러닝 14:50 – 15:50 좌장 : 조규상 (동양대)	딥러닝을 이용한 자동 취약점 분석 이재융, 석재혁, 이동훈 (고려대학교)
	딥러닝 기반 이미지 스팸 검출 방법 연구 이정열, 김형식 (성균관대학교)
	Long Short-Term Memory를 포함한 Autoencoder 기반의 네트워크 침입 탐지 시스템 안선우, 이하윤, 김기열, 김현준, 백윤흥 (서울대학교)
	AI칩과 머신러닝 프레임워크, 암호 구현의 새로운 Tool : 격자 기반 암호를 중심으로 정치곤, 전성일, 백윤흥 (서울대학교)

C5 무선통신 보안 16:00 – 17:00 좌장 : 이동휘 (동신대)	SDR을 활용한 실용적인 LTE 재밍 연구 양호준, 손민철, 노상미, 김용대 (KAIST)
	LTE 제어평면 메시지 암호화에 대한 고찰 손민철, 배상욱, 김홍일, 이은규, 양호준, 이지호, 심규찬, 손수엘, 김용대 (KAIST)
	LTE 무선 접속 과정 취약점에 관한 연구 이은규, 김용대 (KAIST)
	위치기반 키 관리 기법을 적용한 무선센서 네트워크 연구 동향 분석 김종신, 권태경 (연세대학교)

구두발표 트랙 D

TRACK D – 충무관 209A호	
세션	**발표논문**
D1 차량 보안 09:00 – 10:00 좌장 : 유동영 (KISA)	Mixnet 프로토콜을 통한 자율주행차 운영환경 프라이버시 데이터 수집 방안 연구 강기완, 서정택 (순천향대학교)
	2차 Renyi 엔트로피 기반 차량용 침입 탐지 시스템 김광식, 김영식 (조선대학교)
	차량 사이버 보안 가이드 동향 분석 이정호 (한국정보인증)
	CAN 트레이스 정적분석을 통한 데이터 영역의 카운터 필드 식별 방법 연구 김병남, 지청민, 홍만표 (아주대학교)
D2 디지털 포렌식 10:20 – 11:20 좌장 : 김희석 (고려대)	스마트 밴드와 스마트 워치의 디지털 포렌식 사례연구 류지은, 김수빈, 김은주, 장혜지, 최지원, 김종성 (국민대학교)
	안드로이드 애플리케이션 사용 시 저장되는 주요 캐시 데이터 분석에 관한 연구 김형찬, 김동현, 손태식 (아주대학교)
	애플리케이션 디컴파일을 통한 디지털 포렌식 아티팩트 도출에 대한 연구 유동균, 신영훈, 손태식 (아주대학교)
D3 IoT 보안(I) 13:40 – 14:40 좌장 : 강지원 (세종대)	NB-IoT 환경의 제어 영역 프로토콜 분석 툴 개발 및 보안성 분석 심규찬 (KAIST), 박신조 (Technical University of Berlin), 김홍일, 김용대 (KAIST)
	이종 IoT 플랫폼 간 인터워킹을 위한 장치 식별자 기반 관리체계 구자훈, 김영갑 (세종대학교)
	IoT 센서 데이터의 속성기반 암호화를 통한 안전한 서비스 모델 개발 함나연, 김형종 (서울여자대학교)
	IoST 환경에 적합한 LEA 암호알고리즘 최적화 구현 및 성능분석 한주홍, 오진혁, 이재훈, 이옥연 (국민대학교)

구두발표 트랙 D

D4 IoT 보안(II) 14:50 - 15:50 좌장 : 안효범 (공주대)	사물인터넷 디바이스로부터의 서브도메인 디도스 공격을 재귀적 네임서버에서 방어하기 서양진 (㈜코트캔디)
	Z-Wave 보안 취약점 분석 임지환, 조기윤, 성민석, 정영호, 김성범, 김경곤, 이경문 (KITRI BoB), 서화정 (한성대학교)
	로봇청소기 제품군 Attack Surface 분석 방법 임준태, 석지원, 최원빈, 이재휴, 이경수, 안용호, 고영우, 이인형, 이상섭, 이원 (KITRI BoB)
	특정 oneM2M 오픈소스 기반 암호 키관리 기능 분석 김도원, 최은영, 박해룡 (KISA)

D5 5G 보안 연구회 16:00 - 17:00 좌장 : 유일선 (순천향대)	Security management for backhaul-aware 5G-V2X Vishal Sharma, Yongho Ko, Jiyoon Kim, Ilsun You (Soonchunhyang University)
	경매알고리즘기반 분산블록체인마이닝 취약점 분석 김중헌, 신명재, 전주형, 김준희 (중앙대학교)
	차세대 네트워크 시대를 대비한 네트워크 장비의 침해 사례 분석 김완수 (한국교육과정평가원), 신대민 (순천향대학교)
	5G 환경에서의 커넥티드카 서비스를 위한 확장 보안 프레임워크 고병수 (㈜디지캡)

구두발표 트랙 E

TRACK E – 충무관 210호	
세션	**발표논문**
E3 부채널연구회(Ⅰ) 13:40 – 14:40 좌장 : 백유진 (우석대)	부채널 분석 공격에 대응하는 초경량 블록 암호 CHAM 구현을 위한 축소 마스킹 기법 적용 권흥필, 배대현, 하재철 (호서대학교)
	캐시 부채널 공격 방어 기법 연구 전성일, 김기열, 김현준, 이영한, 백윤흥 (서울대학교)
	Intel SGX와 캐시 부채널 공격에 대한 연구 김기열, 이영한, 전성일, 김현준, 백윤흥 (서울대학교)
	캐시 부채널 공격 방법들과 발전에 관한 연구 이영한, 김기열, 방인영, 전성일, 백윤흥 (서울대학교)
E4 부채널연구회(Ⅱ) 14:50 – 15:50 좌장 : 김태현 (SNTWorks)	마이크로아키텍처 부채널 공격기술 연구동향 김태현, 신영주 (광운대학교)
	ChipWhisperer를 이용한 패스워드 기반 인증 방식의 단순 전력 분석 검증 최낙준, 이지은, 김광조 (KAIST)
	선형 연산 특성을 이용한 전력 분석 최적화 방안 박한별, 심보연, 문재근, 한동국 (국민대학교)
	딥러닝을 활용한 부채널 이차 차분분석 성능 향상에 관한 연구 김태성, 최두호 (ETRI)
E5 부채널연구회(Ⅲ) 16:00 – 17:00 좌장 : 문덕재 (삼성SDS)	국산 암호 알고리즘 부채널 분석에 대한 고찰 안규황, 권용빈, 권혁동, 서화정 (한성대학교)
	암호 알고리즘의 연산기반 최적 전력 소모 모델 – Case Study : AES 김주환, 심보연, 한동국 (국민대학교)
	오토인코더 기반 딥러닝을 활용한 부채널 분석 노이즈 제거 기술 연구 권동근, 진성현, 김희석, 홍석희 (고려대학교)

포스터발표 트랙 E

POSTER P1 - 충무관 210호		
세션	번호	발표논문
09:00 - 10:00	1	기계학습 기반의 작성자 분석 기술을 적용한 악성코드 분류 시스템 신건윤, 한명묵 (가천대학교)
	2	HDMI-CEC 프로토콜의 취약점 점검 기법에 대한 연구 김양우, 문창현, 정혜진, 조수연, 조혜원 (KITRI BoB), 양산휘 (세종대학교), 신정훈 (THEORI), 김홍진 (LG CNS)
	3	프로세스 로그 기반의 악성코드 수집 및 탐지 시스템 김동현, 양준호, 김찬진, 염흥열 (순천향대학교)
	4	JSON 기반 원격 절차 호출 프로토콜 퍼징 자동화 이주선 (단국대학교), 박주현 (한세대학교), 이시훈 (아주대학교), 이정민 (세종대학교), 이준오 (고려대학교), 이진우 (서울대학교)
	5	AFL 기반 퍼징 기법에 대한 연구 김현준, 이영한, 양명훈, 김기열, 백윤흥 (서울대학교)
	6	모바일 포렌식 가이드라인 현황 연구 김해니, 권태경 (연세대학교)
	7	Two-Factor 암호화 통한 자료 유출방지 방안 김민창, 김지원 (육군사관학교)
	8	인텔 PT를 활용한 효율적인 수행 흐름 무결성에 대한 연구 서지원, 백세현, 방인영, 김기열, 백윤흥 (서울대학교)
	9	코드 재사용 공격에 대한 조망 방인영, 김현준, 김기열, 백윤흥 (서울대학교)
	10	정적 경로를 이용한 바이너리 프로그램의 함수 식별 방법 김영철, 조은선 (충남대학교)
	11	비정형 위협 데이터 수집 및 연관 분석을 통한 공격 트렌드 분석 박성권 (한동대학교), 장성욱 (순천향대학교), 김종훈 (서울과학기술대학교), 이유정, 김예준 (순천향대학교), 박상호 (㈜크로젠트), 곽경주 (금융보안원)
	12	안드로이드 환경에서의 서드 파티 라이브러리 탐지에 대한 연구 오세라, 김영갑 (세종대학교)
	13	속성 기반 암호화 방식을 이용한 블록에 대한 제한적 접근 서비스 류혜원, 김형종 (서울여자대학교)
	14	IoT 환경에서 타원곡선 암호를 활용한 OAuth 프로토콜 이대휘, 이임영 (순천향대학교)
	15	클라우드 스토리지 환경에서의 Multi-use ID based 프록시 재암호화 김원빈, 이임영 (순천향대학교)
	16	임베디드 펌웨어의 유사 함수식별을 위한 분석 방법 허정민, 김지민, 지청민, 홍만표 (아주대학교)

포스터발표 트랙 E

10:20 – 11:20	17	크롬환경에서의 웹 로그정보를 활용한 개인 성향분석 방법 연구 김지영, 박예원, 안지은, 양지수, 임규희, 김형종 (서울여자대학교)
	18	OpenSSL에서 제공하는 의사난수 API 구조 분석 연구 김현기, 송행권, 이옥연 (국민대학교)
	19	다크웹 악성유저 추적방안에 대한 연구 안상현, 유동민, 정주현, 김만수, 이유진, 김영웅, 이해민 (KITRI BoB)
	20	안드로이드 환경에서의 O2O 서비스 현황 및 보안이슈 문현지, 주완빈, 신지호, 현지산, 정성조, 조민재, 박세한 (KITRI BoB), 이성권 (고려대학교)
	21	소프트웨어 개발 생명주기에서 위협 인텔리전스 적용을 통한 소프트웨어 보안강화 방안 김예준, 류기백, 이유정, 염흥열 (순천향대학교)
	22	DLMS/COSEM 프로토콜을 사용하는 스마트 미터의 취약점에 관한 연구 박준영, 한창현, 피대권, 송상현, 조수민 (한국정보기술연구원)
	23	HastFuzz: 선행 분석 결과 기반의 실행 흐름 유도를 통한 퍼징 방법론 조승현, 이광진, 최광준, 진호용, 나윤종, 박기웅 (세종대학교)
	24	효율적인 악성코드 분석을 위한 에뮬레이션 기반 동적 분석 도구 구현 및 검증 김민재, 임명은, 주하종, 염흥열 (순천향대학교)
	25	민간 클라우드 도입 장애요인 분석을 통한 국방 클라우드 도입 전략 도출 박준규, 전우진 (세종대학교), 이상훈 (국방과학연구소), 박기웅 (세종대학교)
	26	PDF 악성코드 유형분류를 위한 API 시퀀스 정제 방안 연구 김경한, 최보민, 강홍구, 박준형 (한국인터넷진흥원)
	27	탈중앙화 항공 체크인 시스템을 위한 스마트 계약 김혜빈, 박지선, 신상욱 (부경대학교)
	28	자바스크립트 난독화 도구 분석 및 평가 신동순, 김형식 (성균관대학교)
	29	LDA를 이용한 사회공학 공격 산출방안 임승호, 김지원 (육군사관학교)
	30	음성인식 기반 사용자 인증 기술 동향 조사 김베드로, 김형식 (성균관대학교)
	31	An Investigation and Analysis of Blockchain Use Cases for Digital Forensics Sandi Rahmadika, Kyung-Hyune Rhee (부경대학교)
	32	식품 추적 및 제어를 위한 블록체인 솔루션 쵸느에진랏, 이경현 (부경대학교)
	33	머신러닝에 기반한 PE패턴과 악성코드 시각화 분석을 활용하는 분석 방법에 대한 연구 염성규, 신동일, 신동규 (세종대학교)

포스터발표 트랙 F

POSTER P2 – 충무관 211호		
세션	번호	발표논문
09:00 – 10:00	1	사이버 기만을 위한 사이버 기만 트리 모델 박창욱, 김영갑 (세종대학교)
	2	전자적 문서의 법적 효력 향상을 위한 검증방안 연구 -보험회사를 중심으로- 허원석 (고려대학교), 임상헌 (동국대학교), 허재영 (한국교육학술정보원)
	3	중복된 난수 사용을 통한 EC-KCDSA 알고리즘 개인키 추출 방안 고주성, 곽진 (아주대학교)
	4	Performance Analysis of IPsec in Kernel-land and User-land with multi-core implementation Sami Ullah, Joontae Choi, Heekuck Oh (한양대학교)
	5	비콘 기반 서비스의 접근 취약점에 대한 보안 방안 박준영 (대륜고등학교)
	6	가상화폐 거래소 탈중앙화 동향에 관한 연구 조형택, 염흥열 (순천향대학교)
	7	공개툴을 이용한 패턴 기반 보이스피싱 탐지 시스템 탁현주, 임수민, 김민서, 염흥열 (순천향대학교)
	8	카드해킹의 문제점과 대비방안 노무승 (창원중앙고등학교), 이진우 (울산대송고등학교), 이정훈 (울산범서고등학교), 이창엽 (창원경일고등학교), 오현수 (부산진고등학교)
	9	스마트 헬스케어 서비스를 위한 IoT 센서기반 플랫폼 서비스 이원영, 김지영, 강희진, 한수민 (서울여자대학교)
	10	체크리스트 기반 소프트웨어 설계보안 연구 : 소프트웨어 개발보안제도를 중심으로 성선화, 최진영 (고려대학교)
	11	DexGuard 난독화 도구 특성 분석 김규호, 신용구, 이선준, 이정현 (숭실대학교)
	12	의료정보 공유 플랫폼을 위한 하이퍼레저 패브릭 응용 방안 이민기, 민서현, 지청민, 홍만표 (아주대학교)
	13	클라우드 환경에서 CP-ABE 방식을 활용한 안전한 데이터 접근 기법에 관한 연구 황용운, 이임영 (순천향대학교)
	14	블록체인 키 관리서버를 이요한 PGP+ 노창현, 이임영 (순천향대학교)
	15	컨소시엄 블록체인황경에서의 Privacy를 보장하는 안전한 통신시틈에 관한 연구 라경진, 이임영 (순천향대학교)
	16	크로스 아키텍처 바이너리 간 함수 유사도 분석 기법 심규원, 김지민, 지청민, 홍만표 (아주대학교)

포스터발표 트랙 F

10:20 – 11:20	17	효율적인 한국 암호 모듈 검증 제도를 위한 암호 모듈 자동 검증 시스템 박태환 (부산대학교), 안규황, 권혁동, 서화정 (한성대학교), 김호원 (부산대학교)
	18	DQ-Net : 동적 QR 코드 기반 WI-Fi 인증 메커니즘 양유진, 임정현, 최정은, 서화정 (한성대학교)
	19	OpenMP를 활용한 LSH DRBG 병렬 최적 구현 권혁동, 안규황, 서화정 (한성대학교)
	20	파일 고유 식별 정보 기반 통합 유사도 시스템 설계 이동주 (순천향대학교), 강성묵 (강남대학교), 안건우 (대구대학교), 김동욱 (창원과학고등학교), 유기환 (한국디지털미디어고등학교), 이현 (선린인터넷고등학교), 김기홍 (세인트시큐리티), 곽경주 (금융보안원)
	21	취약점 악용 예측에 활용되는 Reference Feature의 적합성 분석 연구 양희동, 이만희 (한남대학교)
	22	Window Stations and Desktops를 활용한 보안 프로그램 활용성에 대한 고찰 여상준, 고동의 (대구대학교)
	23	MITM 공격을 이용한 IoT Hub 환경의 취약점 연구 김지섭, 김동영, 김학진, 방수정, 조진호, 최강현, 임홍렬, 박의성, 지한별 (BoB), 이종호, 이기택 (고려대학교)
	24	망분리 환경에서 불필요 트래픽 제거에 대한 정책연구 Chung Sig Kim, Huy Kang Kim, Sangjin Lee (고려대학교)
	25	Binary Rewriting을 사용한 난독화된 신종 악성코드 식별 시스템 이영전, 한명묵 (가천대학교)
	26	실습형 정보보안 교육 환경 구축 모델에 대한 연구 지한별, 김보경, 윤원석 (라온화이트햇)
	27	AIX 운영체제에서의 엔트로피 측정 및 분석 송행권, 김현기, 이옥연 (국민대학교)
	28	VR 상에서의 안전한 PIN 입력 방법 제안 우재민, 김현준, 김도영, 서화정 (한성대학교)
	29	클라우드 환경에서의 스마트카드를 활용한 개체 인증 개선 방안 조정석, 곽진 (아주대학교)
	30	PwnETH: 이더리움 스마트 컨트랙트 취약점 공격코드 라이브러리 이진우 (서울여자대학교), 김경민 (고려대학교), 정윤서 (한국디지털미디어고등학교), 이진경 (선린인터넷고등학교), 강연호 (거제제일고등학교), 김규현 (고려대학교), 이상섭 (삼성리서치), 김경곤 (고려대학교)
	31	오픈소스 저장소의 데이터를 활용한 가상화폐 프로젝트 유지보수성 평가 최원석, 김형식 (성균관대학교)
	32	비정형 트랜잭션의 비식별 처리 품질 평가 용우석, 이원석 (연세대학교)
	33	로그 기반 변종 악성코드 탐지 방법 조우진, 김형식 (충남대학교)

DATA CHALLENGE

DATA CHALLENGE – 충무관 211호	
세션	**좌장 : 김휘강(고려대)**
CHALLENGE(Ⅰ) 13:40 – 14:40	차량 이상징후 탐지
CHALLENGE(Ⅱ) 14:50 – 15:50	모바일 악성앱 탐지
CHALLENGE(Ⅲ) 16:00 – 17:00	악성코드 탐지

학술대회 등록방법

◉ 등록비

	사전등록		현장등록
	회원	비회원	
정회원/종신회원	80,000원	135,000원	150,000원
학생회원(대학원생)	50,000원	75,000원	90,000원
학부생/고교생	30,000원	30,000원	30,000원

※ 등록자에게는 논문 전체가 수록된 온라인 프로시딩과 중식권 1매 제공됩니다.
(행사 당일 www.cisc.or.kr 에서 다운로드)

- 학회 특별회원사 임직원은 학회 회원으로 준합니다.
  - 학회 홈페이지(www.kiisc.or.kr) → 회원광장 → 특별회원사에서 확인하실 수 있습니다.
- 학부생의 경우, 학생증을 kiisc@kiisc.or.kr 로 송부하시기 바랍니다.
- 등록확인서는 행사 당일 제공해드린 명찰 안에 포함되어 있습니다.

◉ 사전등록

- 사전등록 : 학회 홈페이지 접속 → 학술행사 → 사전등록바로가기 클릭 → 2018 동계학술대회
- 사전등록 송금처
  - 예금주 : 한국정보보호학회
  - 계좌번호 : (국민은행) 754-01-0008-146
- 사전등록시 등록비는 위의 계좌로 송금하시고, 입금자가 대리일 경우 통보 바랍니다.

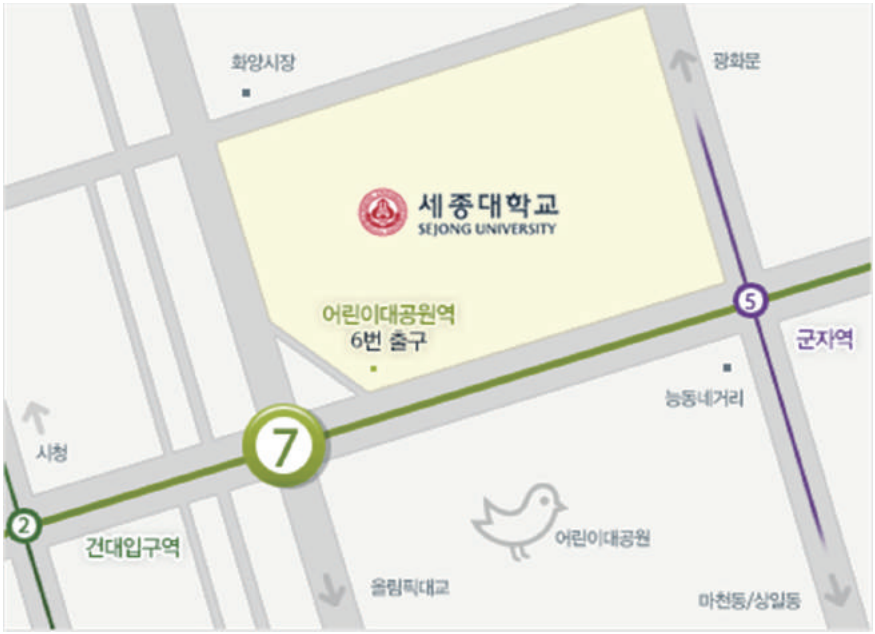
- 논문발표자 사전등록 : 2018년 11월 26일(월)까지
  - 논문발표자의 경우, 사전등록시 논문번호 기재
  - 각 논문당 최소 1명의 저자는 등록해야 합니다. (미등록시 논문 게재목록에서 제외됩니다.)
- 일반참가자 사전등록 : 2018년 12월 3일(월) 오전 11시까지

◉ 문의처

- 행사 문의처 : 02-546-9333(~4) (내선2)
- 계산서 문의 : 02-564-9333(~4) (내선1)

행사장 안내

◉ 세종대학교 캠퍼스 안내



- 주소 : 서울특별시 광진구 능동로 209 (군자동) 세종대학교
- 전화 : 02-3408-3114

◉ 대중교통을 통해 학교로 오시는 방법

지하철

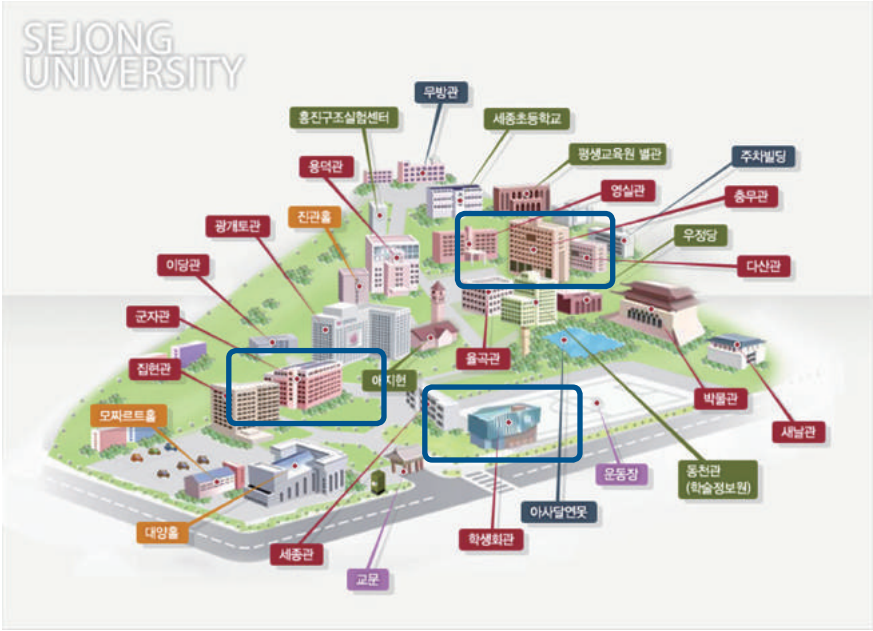
- 2호선 건대입구역이나
- 5호선 군자역에서 환승 후
- 7호선 세종대역(어린이대공원역) 하차 후 6번 출구

시내버스

- 어린이대공원 방향 : 파랑(간선) 721 / 초록(지선) 119, 3216, 4212
- 화양리 방향 : 파랑(간선) 240, 302 / 초록(지선) 2222, 3217, 3220 / 빨강(광역) 102
- 후문(세종초) : 파랑(간선) 240 / 초록(지선) 2012, 2013

행사장 안내

◉ 행사장소



행사장		장 소
충무관	ROOM 209	등록부스 및 다과
	ROOM 202A	Track A (구두발표)
	ROOM 208	Track B (구두발표)
	ROOM 202	Track C (구두발표)
	ROOM 209A	Track D (구두발표)
	ROOM 210	Track E (포스터, 구두발표)
	ROOM 211	Track F (포스터, DATA CHALLENGE)
군자관	소강당(607)	• 개회식 및 정기총회 • 우수논문 및 정보보호 R&D 데이터 챌린지 수상 • 초청강연(암호분야)
학생회관	중식(1F)	• 세트코너

MEMO

한국정보보호학회 동계학술대회

CISC-W'18

Conference on Information Security and Cryptography-Winter 2018

한국정보보호학회

Korea Institute of Information Security & Cryptology