2025년 SECURITY@KAIST 포스터발표

1	Amin Jalilov	Gesture Passwords for VR HMDs
2	Steve Bezalel Iman Gustaman	DetermiFuzz: Program Synthesis for Reproducible Network Protocol Fuzzing
3	Zunnoor Fayyaz Awan	ReCAPD: Repurposing Compilers for Automated Program Diversification
4	고기혁	Towards Universal Disruption of Diffusion-Based Image Inpainting
5	금성호	Private Investigator: Extracting Personally Identifiable Information from Large Language Models Using Optimized Prompts
6	김규연	Towards Acoustic-Based Tagless Object Tracking with Smartwatches
7	김나영	CAMPrints: Leveraging the "Fingerprints" of Digital Cameras to Combat Image Theft
8	김대석	도미네이터 트리를 이용한 맥락 기반 바이너리 보안 패치 유무 검사
9	김동혁	Enabling Timely and Vendor-independent Security Patches in Cellular Networks
10	김세훈	What Makes a Dominator Algorithm Fast? A Study on Binary CFGs
11	김수민	Towards Sound Reassembly of Modern x86-64 Binaries
12	김정현	EVMpress: Precise Type Inference for Next-Generation EVM Decompilation
13	김태은	바람동이 VS 순애보: 지향성 퍼징의 목표 집중형 탐색 전략
14	남호철, 임대현	On the Security Risks of Memory Adaptation and Augmentation in Data-plane DoS Mitigation
15	류연희	확률과 규칙, 친해지길 바래
16	박건	다중 지향성 퍼징으로 여러 군데의 오류 한방에 검사하기
17	박건우	On the Forensic Analysis of LEO Satellites Communications
18	박상준	An Empirical Study on Fuzzing Termination Time
19	박선녀	TrustyMon: Practical Detection of DOM-based Cross-Site Scripting Attacks Using Trusted Types
20	박은찬	STAMP: Synchronized Arrival Time for MEV Prevention
21	서동진	Towards Privacy Preserving Patient State Classification in Psychiatric Seclusion Room using mmWave Radar
22	손민철	Polocolo: A ZK-Friendly Hash Function Based on S-boxes Using Power Residues
23	손진혁	복합 사이버 공격 시퀀스 예측 및 위협 추론 모델
24	송민규	Refusal Is Not an Option: Unlearning Safety Alignment of Large Language Models
25	송주현	CROSS-X: Generalised and Stable Cross-Cache Attack on the Linux Kernel
26	이동재	자연어지만 엄밀한 명세가 되고 싶어
27	이수영	BlurOrigin: Finding UXSS Vulnerabilities in Web Browsers via Property-satisfying Fragment Assembly
28	이정우	On the Applicability of Benford's Law to Detect Saturation in Fuzzing
29	이정호	안티바이러스 성능 허와 실
30	이준학	State-Aware Fuzzing for Satellite Flight Software Using RPNI Mealy-Machine Inference
31	이지현	Weapon Detection in Public Spaces via Metasurface-enhanced mmWave Sensing
32	이진서	When Someone Else's DoS Campaign Becomes Your Deanonymization Opportunity: A Large-Scale, Low-Cost Deanonymization of Tor Onion Services
33	장수진	그 단위 테스트, 정말 다른 거 맞아?
34	전성우	Evaluating-Robustness-of-Reference-based-Phishing-Detectors
35	전준성	AdvPaint: Protecting Images from Inpainting Manipulation via Adversarial Attention Disruption
36	정승일	ML.NET을 활용한 명령어 세트 아키텍처 예측 모델 연구
37	정진	Modeling Voice Phishing Attacks: Design of VP ATT&CK Framework and VP-RTA Matrix
38	정진	이메일 이상 행위 탐지를 위한 시나리오 기반 데이터 모델링 및 AI 모델 설계
39	주현민	Infrared-based Attack on Lane Detection Algorithms for Autonomous Vehicles
40	천은용	User Identification via Behavioral Biometrics Leveraging Smartphone Motion Signal
41	최원지	Design of low-power, high-efficiency acoustic signal attack using amplitude modulation
42	한수진	Automated Attack Synthesis for Constant Product Market Makers

스탬프 채우고 넙죽이 받자!
선물이벤트

각 행사부스에서 스탬프를 받아 아래 칸을 완성하면
넙죽이 키링을 증정합니다!

※ 한정수량으로 선착순 증정

HYUNDAI MOTOR GROUP	SPARROW	Quad Miners
GSIS Graduate School Of Information Security	KAIST Hacking&Security Group GoN	SOMANSA
CSRC Cyber Security Research Center 1	CSRC Cyber Security Research Center 2	CSRC Cyber Security Research Center 3
CyPhyLAB Cyber-Physical Systems and Security Lab 1	CyPhyLAB Cyber-Physical Systems and Security Lab 2	SNS 인증

SNS 2025 SECURITY@KAIST 릴레이 홍보

행사 관련 사진을 인스타그램 스토리 또는
피드에 정보보호대학원(@kaist_gsis)계정을
태그하여 업로드 해주세요!

장바구니 꿈돌이라면 증정

이벤트 선물은
KAIST 정보보호대학원 부스에서 증정해드립니다.

주관 KAIST GSIS 정보보호특성화대학 CSRC Cyber Security Research Center

주최 과학기술정보통신부 KISA 한국인터넷진흥원

2025 SECURITY@KAIST FAIR

"KAIST 교수들 대한민국 보안을 말하다"

KAIST의 우수 보안 연구를 한 자리에서 체험할 수 있는 기회!

2025.08.25 (월) 13시

김병호 · 김삼열 IT융합 빌딩 (N1) 1층

2025 KAIST Hack Quest 본선과 동시 진행됩니다.

2025 SECURITY @KAIST FAIR

행사배치도

101호 키노트 연설 — 차상길 교수
13:00 ~ 13:30

패널 토의 — 강민석 교수
13:30 ~ 14:20

101호 기술세미나 트랙 A

세션 1
좌장 김용대 교수

14:30 ~ 14:55 손수엘 교수
대형언어모델의 안전성과 프라이버시를 점검하는 새로운 Red-teaming 방법론

14:55 ~ 15:20 김용대 교수
셀룰러 이중용도 기술: 감시와 방어 사이의 구조적 딜레마

세션 3
좌장 정동재 연구원 (CSRC)

암호/블록체인 보안

16:20 ~ 16:33 손민철, 이주영 교수님 연구실
Polocolo: A ZK-Friendly Hash Function Based on S-boxes Using Power Residues

16:33 ~ 16:46 박은찬, 강민석 교수님 연구실
Ambush: A Frontrunning Attack in Batch-Order Fair Systems for Blockchains

16:46 ~ 16:59 남호철, 강민석 교수님 연구실
Forky: Fork State-Aware Differential Fuzzing for Blockchain Consensus Implementations

세션 5
좌장 김수민 연구원 (CSRC)

소프트웨어 보안

17:10 ~ 17:23 장봉준, 허기홍 교수님연구실
컴파일러 최적화 버그, 번역 검산과 지향성 퍼징으로 바로 잡아내기

17:23 ~ 17:36 한수진, 윤인수 교수님 연구실
Automatic Attack Synthesis for Constant Product Market Makers (ISSTA '25 paper)

17:36 ~ 17:48 박선녀, 손수엘 교수님 연구실
TrustyMon: Practical Detection of DOM-based Cross-Site Scripting Attacks Using Trusted Types

17:48 ~ 18:00 김수민, 사이버보안연구센터
Towards Sound Reassembly of Modern x86-64 Binaries

참여부스안내

A1	KAIST 정보보호대학원	C1	KAIST CRSC 3
A2	정보보호특성화대학	C2	한준 교수 연구실 1
A3	GoN 동아리	C3	현대자동차
A4	한준 교수 연구실 2	C4	(주)쿼드마이너
B1	KAIST CRSC 1		
B2	KAIST CRSC 2		
B3	(주)스패로우		
B4	(주)소만사		

포스터 발표

A	p1 - p21
B	p22 - p42

117호 데모 및 홍보 부스 전시
14:30 ~ 17:00

연구포스터 전시 관람
15:20 ~ 16:20

114호 기술세미나 트랙 B

세션 2
좌장 허기홍 교수

14:30 ~ 14:55 Ian Oakley 교수
Making Password Checkups Work: Designing for Action, Not Apathy

14:55 ~ 15:20 허기홍 교수
목표 집중형 프로그램 분석

세션 4
좌장 최규현 연구원 (CSRC)

모바일 / 네트워크 보안

16:20 ~ 16:33 이진서, 강민석 교수님 연구실
Tor 익명성 네트워크의 가용성, 익명성 침해 공격 연구

16:33 ~ 16:46 손민철, 김용대 교수님 연구실
Systematic Testing of Context Integrity Violations in Cellular Core Networks

16:46 ~ 16:59 윤종혁, 한준 교수님 연구실
PowDew: Detecting Counterfeit Powdered Food Products using a Commodity Smartphone

세션 6
좌장 고기혁 연구원 (CSRC)

소프트웨어 보안

17:10 ~ 17:23 최규현, 사이버보안연구센터
From Harmful Domain Detection to Criminal Organization Mapping: A Research for Evidence-Based Threat Attribution and Network Analysis

17:23 ~ 17:36 송주현, 윤인수 교수님 연구실
CROSS-X: Generalised and Stable Cross-Cache Attack on the Linux Kernel

17:36 ~ 17:48 송용호, 강병훈 교수님 연구실
Interstellar: 하드웨어 기반 instruction 모니터링을 통한 런타임 보안 위협 탐지 및 사전 차단

17:48 ~ 18:00 고우영, 김용대 교수님 연구실
XAI 기반 LLM 생성 가짜댓글의 언어패턴 분석 및 탐지(XDAC: XAI-Driven Detection and Attribution of LLM-Generated News Comments in Korean