KOREA UNIV SEJONG

AICS News Letter

2025_02.ver

CONTENTS

Vol. 6 | 2025_2.ver

COVER STORY

표지는 인공지능사이버보안학과의 2026 학생회장, 부학생회장의 모습을 담았다.
인공지능사이버보안학과의 새 학생회를 이끌 이 학생들은,
왼쪽 부터 순서대로 김도영, 권호영 이다.

인공지능사이버보안학과 학과장, 한미란 교수님을 만나다.

기술 환경의 변화 속도는 점점 더 빨라지고 있으며, 그에 따라 정보보호가 다루어야 할 문제의 범위 또한 크게 확장되고 있다. 데이터의 규모와 활용 방식이 달라지고, 시스템의 구조가 복잡해질수록 보안 위협 역시 정형화된 형태를 벗어나 새로운 양상으로 나타나고 있다. 이러한 변화에 대응하기 위해, 보안 분야에서도 대량의 정보를 분석하고 위협을 예측할 수 있는 인공지능 기술의 중요성이 점차 부각되고 있다.

인공지능사이버보안학과는 이러한 변화의 한가운데에서 출발한 학과다. 기술의 빠른 진보 속도만큼이나, 무엇을 가르치고 어떤 역량을 길러야 하는지에 대한 고민 또한 끊임없이 이어지고 있다. 학과의 정체성과 교육 철학, 그리고 학생들이 나아가야 할 방향은 단기적인 유행이 아닌 장기적인 시각 속에서 정립될 필요가 있다.

이번 인터뷰에서는 인공지능사이버보안학과 한미란 학과장님과 함께, 학과가 현재 서 있는 위치와 앞으로 지향하는 방향에 대해 이야기를 나눈다. AI·보안 융합 분야의 기술적 흐름에 대한 전망부터, 교육과 연구 전반에 담긴 학과의 고민, 그리고 변화하는 환경 속에서 학생들이 갖추어야 할 태도와 자세까지 폭넓게 담고자 했다.

아래는 한미란 학과장님과의 인터뷰 내용이다.

▲한미란 교수님

Q. 학과장님 본격적인 인터뷰에 앞서, 학과장님에 대한 간단한 소개 부탁드립니다!

A, 안녕하세요. 저는 고려대학교 인공지능사이버보안학과의 교수이자 학과장을 맡고 있는 한미란입니다. **인공지능 기술과 사이버보안의 융합**을 핵심 연구 분야로 삼아, 이론적 기반과 실제 적용을 아우르는 연구와 교육을 진행하고 있습니다. 또한 고려대학교 세종캠퍼스에서 AI Convergence Security Laboratory(AICvS Lab)를 이끌며, 급변하는 **기술 환경 속에서 실질적인 문제 해결 역량을 갖춘 인재 양성**을 목표로 연구 활동을 이어가고 있습니다.

Q. 학과장님께서 바라보는 인공지능사이버보안학과의 현재 위치와 향후 성장 방향, 그리고 장기적인 비전은 무엇인가요?

A, 고려대학교 인공지능사이버보안학과는 **AI기술과 사이버보안을 융합**한 국내 선도 학과로서, 빠르게 변화하는 디지털 신기술 환경에 대응할 AI 보안 전문인재를 양성하는 데 강점을 갖추고 있다고 생각합니다.

특히, **AI기술 기반의 부채널 분석, IoT 보안, 양자기반 암호기술, 첨단 방위산업 기술보안 등** 미래 산업 수요가 높은 분야를 집중적으로 다루며 학문적·산업적 경쟁력을 쌓아가고 있습니다.
앞으로는 **AI기술과 보안 기술을 깊이 이해하는 사이버보안 전문가를 동시에 길러내는 방향**으로 성장할 것이며, 한 산업 분야와의 연계를 통해 실무 역량을 강화할 것으로 기대합니다.
장기적으로는 AI 시대의 새로운 보안 패러다임을 주도하는 교육·연구 중심 허브로 자리잡아, 미래 보안 리더를 배출하는 비전을 가지고 있다고 생각합니다.

Q. 앞으로 AI기술과 보안기술의 융합 분야가 어떤 흐름으로 발전할 것으로 전망하시는지, 그리고 그 안에서 우리 학과 학생들이 특히 준비해야 할 역량과 태도는 무엇일까요?

A, AI기술과 보안기술의 융합은 위협 인텔리전스 자동화, 대규모 보안 데이터 분석, IoT기기의 자율보안 시스템과 같이 **AI 모델이 보안 의사결정을 보조하거나 대체하는 방향**으로 고도화될 것으로 예상됩니다. 또한, 생성형 AI기술을 기반으로하는 사이버 공격과 방어 기술이 동시에 발전함에 따라, 보안 패러다임은 **지속적 학습 기반의 동적 대응 체계**로 전환될 것입니다.

이러한 흐름 속에서 고려대학교 인공지능사이버보안학과 학생들은 머신러닝·딥러닝 등 **AI기술의 원리를 깊이 이해**하는 동시에, 컴퓨터구조•네트워크시스템•암호기술 등 **핵심 보안 분야에 대한 기초 체계와 분석 능력**을 갖추는 것이 매우 중요하다고 생각합니다. 더불어 빠르게 변화하는 사이버위협 환경을 추적하고, 새로운 기술을 능동적으로 탐구하는 태도와 문제 해결 능력이 요구되며, **보안 외 다양한 분야 전문가와 소통할 수 있는 융합적 역량**을 키우길 기대합니다.

이러한 준비를 통해 학생들은 향후 AI기술 기반의 차세대 보안 생태계를 선도하는 핵심 인재가 될 것입니다.

Q. 학과가 추구하는 교육 방향 또는 커리큘럼 구성에서 AI기술과 보안기술의 융합이 어떻게 반영되고 있는지 설명해 주실 수 있을까요?

A, 고려대학교 인공지능사이버보안학과는 보안 전략·관리, 보안위협 운영·방어, 개발·설계, 보안 특수분야로 세분화하여 교육이 진행되고 있으며, 다양한 IT 분야에 수시로 발생하는 보안 문제를 해결하기 위한 AI기술 기반의 보안 전문가를 양성하는 데 초점을 두고 있습니다.

커리큘럼은 머신러닝 • 딥러닝 • 강화학습 • 빅데이터기술 등 **핵심 AI기술 과목**과, 네트워크 보안시스템보안 • 암호기술 • 디지털포렌식 • 통신보안 등 **보안기술 전문 과목**을 균형 있게 배치하여 두 영역을 구조적으로 연결할 수 있도록 설계되어 있습니다. 특히, 최신의 보안 이슈에 대응하기 위한 **실무형 보안기술기반의 캡스톤디자인 교과목**은 협업에서 과제를 수행하고 있는 보안 전문가를 멘토로 구성하여 설계 • 구현 • 검증해보는 경험을 학생들에게 제공하고 있습니다.

산학협력 학부 연구생 제도, 고려대학교 SW중심대학 사업 교내경진대회 참여 등을 통해 학생들이 **실전 보안 문제를 AI 기술로 해결하는 경험**을 쌓도록 지원합니다.

Q. 다가올 기술 환경 변화 속에서 우리 학과가 앞으로 강화하거나 도입하고자 하는 교육·연구 계획이 있다면 소개해주실 수 있을까요?

A, 앞으로 우주 산업이 확장됨에 따라, 사이버보안 분야에서도 **위성체 보안과 우주 통신 보안**은 높은 산업적 기여와 중요한 연구영역으로 자리잡고 있습니다.

CubeSat 기반의 임베디드 보안 실습, LEO 위성 통신에서 발생할 수 있는 재밍 • 스푸핑 공격 분석, 그리고 Space-Air-Ground 통합 네트워크 (Space-Air-Ground Integrated Network, SAGIN)에서의 AI기술 기반의 이상탐지 연구는 학부 수준에서도 충분히 시도할 수 있는 교육 활동이라 판단됩니다.

또한 우주 환경에서의 온보드 AI기술 신뢰성 검증, 양자암호통신 기반 위성 보안 등의 분야도 학습 가치가 크다고 생각됩니다. 이러한 교육과 연구는 학생들이 기존 지상 기반 보안을 넘어서 미래 우주 인프라까지 고려한 확장된 보안 역량을 갖추는 데 도움이 될 것입니다.

Q. 최근 국내·외 보안 이슈 중 가장 주목해서 보신 사례가 있다면 무엇이며, 그 이유는 무엇인가요?

A, 최근 가장 주목할 보안 이슈는 **생성형 AI 알고리즘을 활용한 정교한 사회공학적 • 기술적 공격의 급증**이라고 생각합니다. 실제로 해외에서는 AI 기반 음성 합성으로 기업 담당자를 속여 수백억 원의 자금을 이체하게 한 사례가 보고되었고, 국내에서도 딥페이크 영상과 음성을 이용한 사기 시도 또한 증가하고 있으며, 생성형 AI 알고리즘을 이용한 악성코드 생성 공격 또한 한 축이라고 보여집니다.

이러한 보안 이슈에 관심을 갖고 탐구해야 하는 중요한 이유는 **공격의 속도와 스케일이 AI기술로 인해 비약적으로 확장**되고 있기 때문입니다. 따라서 앞으로의 보안 분야는 기술적 요소뿐만 아니라 사회적 요소까지 포함한 새로운 운영과 대응 프레임워크가 필요하다는 점에 주목해야 한다고 봅니다.

Q. 학생들이 AI기술과 보안기술 연구 수행 또는 산업 진출을 위해 학부 과정에서 경험해보면 좋을 활동(연구, 프로젝트, 학회, 자격, 언어, 독서 등)은 어떤 것이 있을지 조언 부탁드립니다.

A, 학과 교과목으로 편성되어 있는 AI기술과 보안기술 기초과목을 기반으로 하되,
실제 보안 이슈에 접근해볼 수 있는 실전 경험도 매우 중요하다고 생각합니다.

학년 초반에 습득해야 하는 프로그램밍 언어는 학년이 올라갈 수록 능력치를 끌어올리도록 노력해야 하며, 방학 때 이루어지는 현장실습 신청, 연구실 학부연구생이나 프로젝트 학기제에 참여하여 AI기술을 기반으로하는 보안 모델을 구현해보는 것이 큰 도움이 됩니다.

또한, 학과 동아리 (Kuality, KoRec) 참여, 교외 CTF, 해커톤, 아케데미(화이트햇, BoB 등)에 참여하며 실전 감각 익힐 수 있습니다. 학년에 따라 취득할 수 있는 자격증(TOPCIT, 리눅스마스터, 정보처리기사)을 탐색하여 방학동안 기술 스펙을 올릴수 있습니다. 영어 논문 읽기와 최신 연구 트렌드 탐색을 꾸준히 병행한다면 학부 단계에서도 경쟁력 있는 역량을 갖출 수 있습니다.

우리학과 학생들이 수업 이외 경험하면 좋을 활동을 몇 가지 카테고리로 정리해 보겠습니다.

1. 프로그래밍 기술

- 방학 동안 Python, C/C++, Linux 언어 이해 고도화 (1학년 ~ 4학년)

2. 프로젝트 활동

- 매 여름/겨울 방학 동안 신청가능한 현장실습 과목 (3학년 ~ 4학년)

3. 연구 경험

- 교수님 연구실 학부연구생 참여 (2학년 ~ 4학년)
- 프로젝트 학기제를 통한 연구 경험 (3학년 ~ 4학년)

4. 자격증

- TOPCIT (1학년 ~ 4학년)
- 리눅스마스터 (2학년 ~ 4학년)
- 정보처리기사 (4학년)

5. 교외 보안 커뮤니티 및 학과 동아리 참여

- 화이트햇 스쿨& BEST OF THE BEST (BoB)
- 학과 동아리: Kuality, KoRec

6. 외국어 역량
- *영어자격시험*
- *기술 문서를 이해하고 작성할 수 있는 영어 실력*

Q. 마지막으로 학과 학부생 학우들에게 전하고 싶은 메시지가 있다면 부탁드립니다.

A, 제가 학부 과정 학생들에게 전하고 싶은 첫 번째 조언은 **기본에 충실한 공부가 결국 가장 큰 실력이 된다는 것**입니다. 매 수업에 성실하게 임하고, 기초 개념을 제대로 이해하는 것이 앞으로 어떤 진로를 선택하든 흔들리지 않는 기반이 되어줄 것입니다.

또한 4년 동안 '내가 어떤 분야를 좋아하는가, 무엇을 잘할 수 있는가'를 부지런히 탐색하기 바랍니다. 이 과정은 빠르게 결정되기보다는, 각자의 성장 속도에 맞게 여러 경험을 통해 천천히 쌓여가는 것이 더 자연스럽습니다. 다른 학생보다 속도가 느리다고 조급해하지 말고, 앞이 선명하게 보이지 않는 순간이 오더라도 그 자체가 성장의 일부라는 점을 기억하면서 학교 생활을 했으면 합니다.

그리고 가장 강조하고 싶은 것은, **'다른 학생들과 비교하지 않기!!'**입니다. 비교는 자신감을 잃게 만들 뿐이므로, 학기마다 작은 목표를 세우고 실천하는 방향으로 **어제의 나보다 얼마나 내가 나아졌는지에 집중**하며 꾸준히 걸어가길 바랍니다. 마지막으로, 학교 수업 중이든 방학 동안 했던 경험이든 수시과제, 소규모 프로젝트 경험, 현장실습, 동아리 활동 등 다양함 속에서 겪게될 도전과 실패의 기록들을 차곡차곡 쌓아가다보면 나만의 스토리가 자연스럽게 만들어질 것이라 확신합니다.

취재 : 뉴스레터 6기 김주빈('23)

구자훈 교수님 인터뷰

인공지능사이버보안학과 신임 교수
구자훈 교수님에 대해 알아보다.

▲구자훈 교수님

Q. 교수님 자기소개 부탁드립니다.

A, 안녕하세요. 2025년 9월부터 인공지능사이버보안학과에서 함께하게 된 구자훈 교수입니다.
현재 학부와 대학원 강의를 맡고 있으며, 앞으로 학과의 산학·연구 협력 활동에도 적극적으로 참여할 계획입니다. 새로운 환경에서 동료 교수님들, 학생 여러분, 그리고 대학원 연구원 분들과 함께 성장할 수 있기를 기대하고 있습니다.

Q. 교수님의 주요 연구 분야와 관심 분야는 무엇이며, 이 분야를 선택하게 되신 계기는 무엇인가요?

A, 제 주요 연구 분야는 스마트시티와 스마트팩토리와 같은 **사물인터넷 및 사이버-물리 시스템에서의 상호운용성과 보안**입니다.

이기종 센서·플랫폼·서비스 간의 상호운용성과 보안이 확보되지 않으면, 초연결성이라는 궁극적 목표 달성에 제한됩니다. 저는 이러한 사물인터넷·사이버물리 환경에서 상호운용성과 보안이 다양한 도메인으로 적용되기 위한 **필수불가결한 기반 기술**이라고 판단하고, 단순한 기술적 편의가 아니라 서비스의 확장성과 시스템 안전성을 좌우하는 핵심 요소라는 점에 주목해 연구를 이어가고 있습니다. 특히 의미론적·구문론적 정렬과 동적 보안 메커니즘을 중심으로 연구를 지속하고 있습니다.

또한 ISO/IEC 국제표준화 위원으로 활동하면서, 전 세계적으로도 이러한 상호운용성과 보안 기술의 중요성이 크게 대두되고 있음을 체감했고, 이 분야를 더욱 깊이 연구해야겠다는 확신을 갖게 되었습니다.

Q. 현재 진행 중이신 연구나 대표적인 연구 성과가 있다면, 학부생 수준에서 이해할 수 있도록 간략히 소개해주실 수 있을까요?

A, 저는 주로 사물인터넷 환경에서 서로 다른 플랫폼이 타 플랫폼의 기기·자원·서비스를 검색하고 필요한 정보를 요청할 수 있도록 하는 식별체계 기반의 상호운용 기술과, 플랫폼마다 다른 접근제어 정책을 안전하게 연동하는 보안 상호운용 기술을 연구해 왔습니다.

이러한 연구는 스마트시티·스마트팩토리처럼 다수의 이기종 시스템이 포함되는 환경에서 발생하는 문제를 다룬 것으로, **게재연도 JCR(전 세계의 수많은 학술지(논문) 중**에서, 엄격한 심사를 거쳐 선정된 영향력 있고 신뢰도 높은 '우수 국제 학술지'를 분류하는 기준) **Top 1%권 SCIE 저널 게재, 우수 국제학술대회 발표, 미국 특허 등록, 국제표준 제정 등으로 우수성을 인정**받았습니다.

Q. 앞으로의 연구 계획과 중·장기적인 목표에 대해 말씀해주실 수 있을까요?

A, 향후 연구에서는 사이버-물리 시스템 보안과 이기종 시스템('서로 다른 종류'라는 뜻으로, 하드웨어 구조나 통신 프로토콜 등이 달라 원래는 호환되기 어려운 다양한 시스템들이 섞여 있는 환경) 간 상호운용을 AI 기반으로 고도화하는 데 중점을 두고자 합니다.
특히 플랫폼 간 속성·정책 차이를 **AI가 자동으로 분석·매핑하는 지능형 접근제어 및 보안 자동화 기술**을 개발하여, 관리자가 직접 개입하지 않아도 되는 **자가-적응형 보안 체계**를 실현하는 것이 목표입니다.

중기적으로는 이러한 기술을 **스마트 환경과 산업용 IoT**에 적용하여, 실제 도메인에서도 안전하고 효율적인 운영이 가능하도록 하는 완전 자동화 기반의 상호운용·보안 프레임워크를 구축하고자 합니다.
장기적으로는 **국제표준화 활동과 연계**하여 이러한 연구들이 글로벌 스마트 환경 보안의 기반 기술로 자리 잡을 수 있도록 기여하고 싶습니다.

Q. 학부에서 어떤 과목들을 주로 강의하고 계신지, 간단히 소개 부탁드립니다.

A, 학부에서는 **컴퓨터구조설계및이론**과 **강화학습** 과목을 강의하고 있으며,
다음 학기에는 **소프트웨어공학** 및 **AI와데이터거버넌스** 과목을 개설해 학생들과 함께할 예정입니다.

Q. 강의를 개설하실 때 특히 중요하게 생각하시는 교육 철학이나 원칙이 있으신가요?

A, 강의를 설계할 때 가장 중요하게 생각하는 점은, 기술이나 코드를 무분별하게 익히는 태도보다 그 기술이 어떤 목적과 원리로 동작하는지를 이해하는 것입니다.
AI나 보안 분야에서는 도구 사용 자체보다 **왜 이 기술을 쓰는가**, **어떤 문제를 해결하려는가**를 명확히 이해하는 것이 훨씬 중요하다고 생각합니다.

그래서 수업에서도 개념적 이해, 원리 기반 학습, 기술 적용으로 이어지는 구조를 지향하며, 기술 중심의 표면적 학습보다는 문제를 바라보는 사고력과 개념적 깊이를 강조하고 있습니다.

Q. 학생들과의 수업, 연구, 상담 과정에서 가장 중점을 두고 계신 부분은 무엇인가요?

A, 수업, 연구, 상담에서 제가 가장 중점을 두는 부분은 문제의 핵심을 정확히 짚고, 무엇이 정말 어려운 부분인지 함께 파악하는 것입니다. 수업에서는 단순히 내용을 전달하기보다 **이 문제가 본질적으로 무엇을 묻는가**, **어디가 중요한 지점인가**를 중심으로 설명하려고 합니다.

연구를 지도할 때도 기술 구현보다 먼저 **현황과 상황을 분석하고 핵심 포인트를 찾는 과정**을 가장 중요하게 생각합니다. 상담에서는 학생이 겪는 어려움이나 진로 고민에서 우선 **무엇을 먼저 정리해야 하는지 함께 살펴보는 방향**으로 접근하고 있습니다.

Q. 인공지능·사이버보안 분야를 준비하는 학부생들이 꼭 갖추면 좋겠다고 생각하시는 기본 역량이나 태도가 있다면 무엇일까요?

A, 분야와 상관없이 학생분들에게 가장 중요한 것은 **성실성과 꾸준함**이라고 생각합니다.

두 번째로는, AI와 사이버보안처럼 변화 속도가 빠른 분야에서는 새로운 기술을 받아들이고 계속해서 배워 나갈 수 있는 **적응력과 학습력**도 필요합니다.

마지막으로, 작은 설정이나 데이터의 미세한 차이가 결과에 큰 영향을 줄 수 있는 분야이기 때문에, 실제 구현과 분석 과정에서는 **섬세하고 꼼꼼한 태도**가 도움이 됩니다.

Q. 교수님께서 바라보시는 인공지능사이버보안학과의 강점은 무엇이라고 생각하시나요?

A, 인공지능사이버보안학과의 가장 큰 강점은 **산업 수요가 매우 높은 두 분야**, AI와 보안이 교차하는 특화된 교육과 연구를 제공한다는 점이라고 생각합니다. 또한 **다양한 연구 배경과 전문성을 가진 교수님들**이 함께 계셔서, 학생들이 여러 분야를 접해보고 자신의 진로에 맞는 방향을 선택할 수 있는 폭이 넓다는 점도 큰 장점입니다.

학교에 와서 특히 느낀 점으로는, **학부생들을 대상으로 한 지원과 활동이 풍부하고 체계적**이라는 점인데, 학생들이 실습·프로젝트·경진대회·연구 참여 등 다양한 기회를 경험할 수 있다는 것이 학과의 경쟁력이라고 생각합니다.

Q. 인공지능사이버보안학과가 앞으로 어떤 방향으로 발전해 나가야 한다고 보시는지, 학과에 대한 교수님의 비전이 궁금합니다.

A, 인공지능사이버보안학과에 와서 느낀 점은, AI와 보안이라는 두 분야가 실제 산업에서도 점점 더 깊이 연결되고 있다는 흐름과 학과의 방향이 잘 맞아떨어진다는 것이었습니다. 앞으로도 단순히 두 분야를 따로 배우는 수준을 넘어서, **AI 기반 보안이나 안전한 AI와 같이 실제 문제를 해결할 수 있는 융합형 역량**이 더욱 중요해질 것으로 생각합니다.

그래서 학과도 이러한 부분을 중심으로 교육과 연구의 폭을 조금씩 넓혀갈 수 있다면 학생들에게 더 큰 기회를 줄 수 있을 것이라 느꼈습니다. 저 역시 IoT·스마트시티·CPS 보안과 같은 제 연구 분야를 바탕으로 학과의 이런 융합적 방향에 기여하고, 함께 성장할 수 있기를 기대하고 있습니다.

Q. AI와 보안이 융합되는 현재 흐름 속에서, 관련 산업 및 진로 전망을 어떻게 보고 계신지, 학부생들에게 현실적인 조언을 들려주신다면요?

A, AI와 보안의 융합은 실제 산업 환경에서도 여전히 해결해야 할 과제가 많은 어려운 주제입니다. AI가 다양한 분야에서 자동화를 빠르게 확산시키고 있지만, 보안 영역에서는 최종 관리자의 판단과 책임을 완전히 대체하기 어려운 특성이 있습니다.

그렇기 때문에 앞으로는 **AI가 보안을 보조하고, 보안은 AI의 안전한 활용을 보장하는 형태의 실질적 융합 역량**이 더욱 중요해질 것으로 보고 있습니다. 학부생 분들도 이러한 흐름을 이해하고 꾸준히 준비한다면, AI·보안은 물론이고 스마트시티, 산업자동화 등 매우 다양한 분야에서 커리어를 확장하고 중요한 역할을 할 수 있을 것이라 생각합니다.

Q. 연구실(또는 랩)에 소속되어 활동하고 싶은 학생들이 어떤 준비를 하면 좋을지, 함께 일하고 싶은 학생상(학생에게 기대하는 점)을 말씀해주실 수 있을까요?

A, 연구실에서 가장 우선시하는 점은 **성실함**과 **꾸준함**입니다.

한 번 실패했다고 포기하기보다, 그 이유를 찾고 꾸준히 다시 해보려는 태도가 중요하다고 생각합니다.
또한 저는 연구실 멤버들과 잘 어울릴 수 있는 공동체성을 매우 중요하게 봅니다.
연구는 혼자 잘하는 것보다 팀으로 협업해야 하는 경우가 훨씬 많습니다. 실제로 혼자서 똑똑한 사람은 많지만, 구성원들과 조화를 이루며 함께 성장할 수 있는 능력이 더 큰 가치가 있습니다.

성적은 크게 중요하게 보지 않습니다. 저 역시 학부 시절 성적이 우수한 편이 아니었습니다 ^^;

무엇보다 앞서 말한 **성실함**과 **공동체 의식을 갖추기 위해 노력하는 모습**을 더 중요하게 생각합니다.

취재 : 뉴스레터 6기 고건우('25)

2025학년도 2학기,
다시 모인 우리의 자리
인공지능사이버보안학과 개강총회

개강 후 공기가 서서히 식어가던 어느 날 저녁, 인공지능사이버보안학과 학생들이 한자리에 모였습니다. **2025학년도 2학기 개강을 알리는 개강총회**가 열리며, **학과의 또 하나의 시작을 함께 맞이**했습니다.

2학기 개강총회는 한 학기를 함께 보낸 재학생들이 다시 모여 서로의 안부를 나누고, 다가올 학기를 준비하는 자리로 마련되었습니다. 행사 시작 전부터 곳곳에서는 오랜만에 만난 학우들의 반가운 인사와 웃음소리가 이어졌고, 학우들의 표정에는 자연스러운 설렘이 묻어났습니다.

개강총회 시작 후, **교수님들께서는 학우들에게 응원의 메시지**를 전하며, 학업뿐 아니라 학과 생활 전반에 대해 따뜻한 조언을 건넸습니다. 특히 일방적인 전달이 아닌, 먼저 다가와 학생들과 눈을 맞추며 소통하는 시간이 이어졌다는 점에서 더욱 의미가 깊었습니다.

이후에는 자유롭게 이야기를 나누는 시간이 이어졌습니다. 종강 이후의 근황을 나누는 대화부터 선후배 간의 전공 수업과 진로에 대한 고민까지, 다양한 대화가 자연스럽게 오갔습니다. 이 과정에서 **학우들은 서로에게 힘이 되는 조언**을 주고받으며 **학과 공동체로서의 유대감**을 다시 한 번 느낄 수 있었습니다.

이번 2025학년도 2학기 개강총회는 학기 초 학과 구성원들이 서로를 다시 마주하고, 앞으로의 시간을 함께 준비하는 뜻깊은 자리로 마무리되었습니다. 학과 구성원들이 서로의 이야기에 귀 기울이며, 학과 공동체로서의 유대감을 다시 한 번 느낄 수 있었던 시간이었습니다.

취재 : 뉴스레터 6기 심재규('24)

인공지능사이버보안학과 학생회장 인터뷰

2026학년도 학생회를 이끌어갈 리더

11월 20일부터 21일까지 총 이틀간 진행된 학생회장 선거를 통해, 2026학년도 학생회장으로 22학번 김도영 학우가 선출되었다. 김도영 학우는 '화합'이라는 이름의 학생회를 통해 학과 구성원 모두가 하나로 이어질 수 있는 공동체를 만들어가겠다는 포부를 밝혔다. '화합'은 과거와 현재, 미래의 학우들이 함께 어우러져 학과의 가치를 이어간다는 의미를 담고 있으며, 이를 바탕으로 소통과 연대를 중심에 둔 학생회 운영을 목표로 하고 있다. 이번 인터뷰에서는 김도영 학우를 만나, 2026학년도 학생회의 방향성과 학생회장으로서의 각오에 대해 자세히 들어보았다.

▲제 10회 학생회장 김도영

Q. 간단한 자기소개와 출마하게 된 계기

A, 안녕하세요, 이번 인공지능사이버보안학과
제 10대 학생회장에 당선된 **22학번 김도영**입니다.
2025년 학생회 활동을 하며 좋은 학우들과 교류할 수 있었고, 학과 행사를 직접 기획하고 실행해 나가는 과정이 저에게는 매우 의미 있는 경험이었습니다.

이러한 경험을 통해 **학생회 활동의 중요성**을 느끼게 되었고, 내년에도 다른 자리에서 새로운 경험을 쌓으며 **학과를 위해 일해보고 싶다는 생각**으로 출마하게 되었습니다.

Q. 학생회장으로서 가장 중요하게 생각하는 것은 무엇인가요?

A, 제가 학생회장으로서 가장 중요하게 생각하는 것은 **'관계'**입니다. 한 번뿐인 학교생활 속에서 학우 여러분이 **서로 좋은 관계를 만들어가며 의미 있는 시간**을 보냈으면 좋겠다고 생각합니다. 수업이나 행사뿐만 아니라 일상 속에서 자연스럽게 이어지는 관계가 학교생활의 만족도를 크게 좌우한다고 느꼈기 때문입니다.

또한 학생회 내부에서도 마찬가지로 관계가 중요하다고 생각합니다. **학생회는 영리를 추구하는 단체가 아닌 만큼**, 성과보다도 서로를 배려하고 이해하는 태도가 우선되어야 한다고 생각합니다. 각자의 역할을 존중하며 양보하고 협력하는 분위기 속에서 운영되는 학생회가 되어야만, 그 에너지가 학우들에게도 긍정적으로 전달될 수 있다고 믿습니다. 이러한 관계를 바탕으로, **모두가 편하게 소통하고 신뢰할 수 있는 학생회**를 만들어가고 싶습니다.

Q. 학우들에게 약속드리고 싶은 변화와 개선점이 있나요?

A, 구체적인 수치나 정량적인 목표를 제시하기보다는,
학우들이 학교생활 속에서 **자연스럽게 체감할 수 있는 변화**를 만들어가는 데에 중점을 두고 싶습니다.

먼저, **신입생들이 학과와 학교생활에 보다 쉽게 적응**할 수 있도록 도움을 주고자 합니다.
학과 생활이 낯설 수 있는 신입생들이 부담 없이 학과에 적응하고, 선후배와 자연스럽게 소통할 수 있는 환경을 만드는 것이 중요하다고 생각합니다.

또한, 학우들 간의 교류가 더욱 활발해질 수 있도록 **다양한 소통의 장**을 마련하고 싶습니다.
단순히 행사를 진행하는 데에 그치지 않고, 학우들이 '서로 더 친해졌다'고 느낄 수 있는 경험을 제공하는 것이 목표입니다.

마지막으로, 지난해 학생회 간부들이 올해도 많이 이어지는 만큼, **기존의 경험과 노하우**를 잘 살려 학과 행사들이 보다 안정적이고 매끄럽게 진행될 수 있도록 노력하겠습니다.

Q. 학생회장에 당선된 소감 한마디 부탁드립니다.

A, 먼저 저를 믿고 지지해 주신 모든 학우 여러분께 진심으로 감사드립니다.
그만큼 큰 책임감을 느끼고 있으며, 앞으로의 1년 동안 학우 여러분이 '좋은 학과에서 의미 있는 한 해를 보냈다'고 느낄 수 있도록 최선을 다해 노력하고 헌신하겠습니다.

부족한 점도 있겠지만, **항상 열린 자세로 소통하며 더 나은 학과**를 만들어가겠습니다.
앞으로의 1년, 잘 부탁드리겠습니다.

취재 : 뉴스레터 6기 심재규('24)

인공지능사이버보안학과의 배움의 장,

제 2회 학술제 수상팀 인터뷰

인공지능과 사이버보안이라는 두 핵심 기술 영역은 더 이상 분리된 개념이 아니다.
인공지능 기술의 확산은 새로운 보안 위협을 낳는 동시에, 이를 대응하기 위한 보안 기술의 진화를 요구하고 있다. 이러한 흐름 속에서 인공지능사이버보안학과는 **학문적 탐구를 넘어 실제 문제 해결로 이어지는 연구와 프로젝트를 지속적으로 장려**해 왔다.

이번 인공지능사이버보안학과 제2회 학술제는 이러한 학과의 방향성을 분명히 보여주는 자리였다.
수상 팀들은 단순한 이론 제시에 그치지 않고, 현실의 보안 문제를 인공지능 기술로 분석·해결하고자 한 명확한 문제의식과 창의적인 접근을 선보였다.

이번 인터뷰에서는 **학술제에서 우수한 성과를 거둔 학년별 수상 팀을 대상**으로 프로젝트의 기획 배경과 핵심 아이디어, 연구 및 구현 과정에서의 고민, 그리고 향후 발전 방향에 대해 이야기를 나누고자 한다.

인공지능과 보안의 접점에서 새로운 가능성을 모색한 이들의 경험은, **같은 분야를 고민하는 학과 구성원들에게 의미 있는 참고 사례**가 될 것이다.

아래는 학술제 학년별 수상 팀 팀장과 진행한 인터뷰이다.

Q. 안녕하세요! 우선 팀에 대해서 간단하게 소개해주실 수 있나요?

최장우 (1학년 팀) > 안녕하세요. 현재 나라의 부름으로 인해 군휴학 중인 24학번 최장우입니다.
저희 팀은 저와 25학번 윤다현 학우, 총 2명으로 구성되어 있습니다.

조준하 (2학년 팀) > 안녕하세요. 22학번 조준하입니다.
저희 팀은 저와 24학번 양희지 학우가 팀을 이뤄 학술제에 참여하였습니다.

임건형 (3학년 팀) > 안녕하세요. 저는 팀장을 맡고 있는 20학번 임건형입니다.
팀원으로는 23학번 이명현, 김누리한, 김주빈 학우와 25학번 신민규 학우, 총 5명으로 이루어져 있습니다.

권희진 (4학년 팀) > 안녕하세요! 저희 팀 '깜몽이 요리사'는 저와 22학번 이창민, 정다은, 정수진 학우, 23학번 김주빈 학우로 구성된 연구팀입니다. 저는 22학번 권희진으로, 본 연구팀 팀장을 담당했습니다.

Q. 이번 학술제에서 발표하신 연구(또는 프로젝트)의 주제와, 해당 주제를 선택하게 된 계기는 무엇인가요?

최장우 (1학년 팀) > 이번 학술제에서 발표한 주제는 **JavaScript 오픈소스 상에 존재하는 취약점 발견을 자동화하기 위해 커버리지 측정과 AI 코드 오디팅을 결합한 자동화 탐지 도구**입니다.
AI 기술의 발전으로 기존에는 많은 시간과 비용이 필요했던 작업들을 효율적으로 보완할 수 있게 되었고, 이를 기존 취약점 탐색 방법론과 결합한다면 오픈소스 코드 상의 취약점을 보다 효과적으로 탐지할 수 있을 것이라고 판단하여 해당 주제를 선택하게 되었습니다.

조준하 (2학년 팀) > 이번 학술제에서는 **AI를 활용한 문서형 악성코드 탐지**라는 주제로 참여하였습니다.
이번 학기에 한미란 교수님의 '인공지능개론' 수업을 수강 중인데 해당 수업에서 배운 내용을 악성코드 탐지에 접목시킬 수 있을 거 같아 해당 주제로 연구를 시작하게 되었습니다.

임건형 (3학년 팀) > 저희 프로젝트 주제는 **LLM(MCP) 기반 웹 취약점 스캐너 개발**입니다.
KUality 인원들과 현재 진행 중인 프로젝트이기도 해서, 학술제를 통해 공유하고 알리고자 이 주제로 참여하게 되었습니다.

권희진 (4학년 팀) > 저희 연구 주제는 **CAPTCHA Solver 공격 전략 분석 및 대응 CAPTCHA 모델 설계**입니다.
최근 CAPTCHA Solver가 상용·오픈소스 형태로 널리 확산되면서, 계정 자동 생성, 스팸 유포, 투표 시스템 조작, 무단 웹 스크래핑과 같은 악의적 행위가 현실적인 사회 문제로 나타나고 있습니다.
기존 CAPTCHA가 여전히 사용되고 있음에도 불구하고, 실제로는 이미 자동화된 해석 모델에 상당 부분 무력화되어 있다는 점에서 문제의식을 느꼈고, 이를 보완할 수 있는 새로운 CAPTCHA 설계 방향을 제안하고자 해당 주제를 선택했습니다.

Q. 연구를 통해 해결하고자 했던 핵심 문제는 무엇이며, 이를 해결하기 위해 제안한 핵심 아이디어나 접근 방식은 무엇인가요?

최장우 (1학년 팀) > 본 연구의 목표는 단순히 취약점 하나를 찾는 것이 아니라, **오픈소스 상에 존재하지만 아직 공개되지 않은 취약점을 발견할 수 있는 도구를 만드는 것**이었습니다. 이를 위해 프로젝트 초기 단계에서 사용 가능한 도구, 분석 대상이 될 오픈소스, 테스트 환경 등을 정리하는 데 많은 시간을 투자했습니다.
다만 **개발 기간이 한정**되어 있었기 때문에 모든 것을 시도하기보다는, 주어진 시간 안에 가장 **현실적으로 결과를 낼 수 있는 방향을 기준으로 우선순위를 설정**했습니다. 기존에 이미 검증된 정적 분석, 동적 분석, 퍼징, 그래프 탐색 기법들을 단순히 새로 만드는 대신, 상황에 맞게 조합하여 하나의 흐름으로 구성하는 방식을 택했습니다. 특히 각 도구가 만들어내는 결과를 어떻게 다음 단계에서 활용해 의미 있는 결과로 연결할 것인지에 초점을 맞췄고, 여러 테스트베드를 구축하여 아이디어를 검증했습니다.
또한 **자동화와 사람의 판단 사이의 균형을 중요**하게 보았으며, 자동으로 후보를 추려내되 최종 검증은 사람이 수행하도록 설계하여 오탐을 줄이는 것을 핵심 과제로 삼았습니다.

조준하 (2학년 팀) > 문서형 악성코드는 정상 문서와 겉보기에는 크게 다른점이 없어 사용자를 쉽게 속일 수 있다는 문제점이 있습니다. **문제 해결을 위해 실제 문서형 악성코드 샘플을 수집**하여 **RandomForest 알고리즘으로 정상 / 악성 여부를 알지 못하는 문서를 판별하는 연구**를 진행하였습니다.

임건형 (3학년 팀) > 핵심 문제는 취약점 후보를 많이 뽑더라도 실제로 위험한지, 어떻게 고쳐야 하는지까지 이어지지 않으면 실무적으로 도움이 떨어진다는 점이었습니다.
그래서 저희는 **LLM이 코드 문맥을 종합적으로 추론**해 취약성 판정, 유형 분류, PoC 개념 정리, 패치 권고까지 제시하는 **문맥 기반 파이프라인**을 구상했습니다.

권희진 (4학년 팀) > 먼저, **CAPTCHA Solver의 원리**를 먼저 확인하고, 이를 **회피하는 방식을 도입**하려고 하였습니다. 대표적으로 Solver는 CAPTCHA의 이미지를 OCR을 통해서 글자를 인식하고 이를 텍스트로 변환하는 방식을 사용하기 때문에 텍스트의 주변 경계를 국소적으로 조작하는 방식을 사용하였습니다.
이때, 색상과 경계, 주파수를 주기적으로 변화하는 방식을 사용하였고, 이에 더해 공진/공명, 착시, 등휘도 효과도 추가하였습니다. **이미지를 인식할 때**, 이미지를 주파수로 변환하는 **Fourier transform을 사용한다는 점을 이용**해서 주파수 변환을 주로 연구하였습니다.
추가적으로 배경을 글자와 반대로 이동시키고, 속도도 다르게 하는 방법, 시공간적으로 CAPTCHA를 변화시키는 방법도 추가적으로 연구하였습니다.

Q. 기존 연구나 기술과 비교했을 때, 이번 연구가 갖는 차별점이나 새롭게 시도한 요소는 무엇이라고 생각하시나요?

최장우 (1학년 팀) > 기존 연구나 기술과 비교했을 때 이번 연구의 가장 큰 차별점은 **커버리지 기반 실행 흐름 분석과 AI 코드 오디팅을 하나의 자동화 파이프라인으로 결합**했다는 점입니다.
많은 기존 도구들이 단일 기법에 집중하는 반면, 본 프로젝트는 이미 존재하는 도구들을 어떤 순서로, 어떤 기준으로 연결할 것인지에 집중하여 실용적인 자동화 구조를 설계했습니다.

조준하 (2학년 팀) > 기존 악성코드 탐지 방식은 주로 시그니처 기반으로 이미 알려진 악성코드만 탐지할 수 있다는 한계가 있었습니다. 저희 연구는 **문서를 실행하지 않고 정적 분석만을 분석해 악성 여부를 판별할 수 있다는 점**에서 차별화됩니다. 특히 olevba를 활용해 176개의 구조적 특징을 자동으로 추출하고, 이를 AI 모델에 학습시켜 기존 방식으로는 놓칠 수 있는 악성 문서도 탐지할 수 있도록 설계했습니다. 또한 단순히 악성 여부만 판별하는 것이 넘어 공격 유형까지 분류하려고 시도한 점도 의미가 있다고 생각합니다.

임건형 (3학년 팀) > 기존 스캐너들은 규칙 기반 / 키워드 기반이라 이게 진짜 취약점인지 애매한 경우가 꽤 많았습니다.
저희는 단순히 의심에서 끝나는 게 아니라, **코드 문맥을 함께 보고 왜 위험한지, 어떤 조건에서 발생하는지, 어디를 어떻게 고치면 되는지까지 자연스럽게 연결해서 보여주려는 점**을 차별점으로 잡았습니다.
한마디로, 탐지 자체보다 판단 + 설명 + 수정 방향에 더 초점을 둔 방식입니다.

권희진 (4학년 팀) > 기존의 정부 24, 대법원 '나의사건검색', 경찰청 '순찰신문고'와 같은 주요 공공기관에서는 CAPTCHA에 실선을 추가하여 인식을 저하시키거나 기울기를 다르게 하는 간단한 방식으로 CAPTCHA를 적용하였습니다.
이러한 간단한 방식으로 생성된 CAPTCHA는 오픈소스로 이루어진 CAPTCHA Solver들에 의해 쉽게 해석이 가능했습니다. 이와는 다르게 **무겁지 않은 연산 방식과 차별화된 방식으로 생성**한 해당 연구의 CAPTCHA의 경우 이러한 **공공기관에서 활용하고 있는 CAPTCHA와 차별점**을 갖고 있습니다.

Q. 이번 학술제를 통해 얻은 주요 성과나 결과를 간략히 정리해 주신다면 어떤 점을 들 수 있을까요?

최장우 (1학년 팀) > 이번 학술제를 통해 얻은 주요 성과는 개념 수준에 머물러 있던 아이디어를 실제로 동작하는 구조로 구현했다는 점입니다. 커버리지 수집부터 탐색 경로 선별, AI 기반 코드 분석, 그리고 사람에 의한 최종 검증까지의 흐름을 하나의 실험 환경에서 반복 가능하게 만들었고, 이를 통해 실제 오픈소스 코드에서 의미 있는 취약점 후보를 도출할 수 있었습니다.

조준하 (2학년 팀) > 정상/악성 문서 판별에서 테스트 데이터 기준 99.77%의 정확도를 달성했습니다. 이는 실제로 사용 가능한 수준의 높은 탐지율이라고 생각합니다. 다만 공격 유형 분류에서는 F1-score가 0.1389로 낮게 나왔는데, 이는 데이터 불균형과 일부 문서가 'unknown'으로 분류된 점이 원인으로 분석됩니다. 이러한 한계점을 명확히 파악한 것 자체도 중요한 성과라고 생각합니다.

임건형(3학년 팀) > 가장 큰 성과는 프로젝트를 실제로 돌아가는 형태로 만들어 수집 → 분석 → 결과 정리까지 전체 흐름을 잡았다는 점입니다. 또한 결과를 단순 텍스트로 나열하는 방식이 아니라 JSON 형태로 정리해 자동으로 누적되고 비교도 가능하게 만들었습니다. 발표를 준비하면서도 단순 데모에 그치지 않고, 실제로 계속 확장해서 활용할 수 있는 구조를 만들기 위해 노력했습니다.

권희진 (4학년 팀) > CAPTCHA는 단순한 보안 요소라고 생각해왔지만, 실제로는 매우 다양한 Solver들이 이미 존재하고 있다는 점이 인상 깊었습니다.
또한, 시각 인지·주파수 분석과 같은 다른 도메인의 개념을 보안 문제에 적용했을 때 새로운 접근이 가능하다는 점을 직접 확인할 수 있었습니다. 이 경험을 통해, 보안 문제를 단일 기술이 아니라 구조적 관점에서 바라보는 시각이 중요하다는 것을 배울 수 있었습니다.

Q. 연구 결과가 실제로 적용된다면, 특정 분야(산업·연구·사회)에 어떤 방식으로 기여할 수 있을 것이라고 보시나요?

최장우 (1학년 팀) > 연구 결과가 실제로 적용된다면 **오픈소스 보안 감사, 기업 내부 라이브러리 점검, 보안 연구자의 초기 분석 단계 등에서 활용될 수 있을 것**으로 생각합니다.
사람이 직접 코드를 모두 분석해야 했던 부담을 줄여주고, 보안 인력이 더 중요한 판단과 검증 작업에 집중할 수 있도록 기여할 수 있을 것입니다.

조준하 (2학년 팀) > 기업이나 공공기관의 이메일 보안 시스템에 적용될 수 있을 것 같습니다.
문서 탐지 모델을 이메일 첨부파일 검사 시스템에 적용한다면 사전에 악성 문서를 차단할 수 있습니다.
특히 문서를 실행하지 않고 정적 분석만으로 판별하기 때문에 안전하고 빠른 검사가 가능합니다.

임건형 (3학년 팀) > 실무에서는 취약점 존재 여부만 확인하고 끝나는 게 아니라, 결국 수정까지 이어져야 합니다. 저희가 노린 기여도 바로 그 부분입니다. 개발자나 보안 담당자가 결과를 보고 바로 수정 방향을 잡을 수 있도록 **근거와 맥락을 함께 제공**하면 대응 속도가 확실히 빨라질 수 있다고 생각합니다.
특히 플러그인처럼 코드가 방대하고 품질이 들쑥날쑥한 환경에서는, 우선순위를 잘 잡고 위험한 것부터 처리하는 데 도움이 될 것 같습니다. 개인적으로는 **버그 헌팅**을 할 때도 유용하게 활용할 수 있을 것 같습니다.

권희진 (4학년 팀) > 본 연구 결과는 정부·공공기관뿐만 아니라, 회원가입이나 인증 절차에서 CAPTCHA를 **사용하는 모든 웹 서비스 전반에 적용 가능**하다고 생각합니다. 특히 자동화 공격으로 인한 서비스 신뢰도 저하나 운영 비용 증가 문제를 완화하는 데 기여할 수 있을 것으로 기대합니다.

Q. 현재 결과를 바탕으로 향후 연구를 어떤 방향으로 확장·발전시켜 나가고 싶은지 궁금합니다.

최장우 (1학년 팀) > 향후 연구에서는 AI가 단순히 취약점 후보를 제시하는 것을 넘어, **해당 코드가 왜 위험한지, 어떤 조건에서 취약점이 발생하는지**를 보다 명확하게 설명할 수 있도록 발전시키고 싶습니다. 또한 JavaScript 외의 다른 언어 생태계로 확장하거나, CI 환경과 자연스럽게 연동되는 형태로 발전시키는 것도 고려하고 있습니다.

조준하 (2학년 팀) > 포스터에 기재한대로, Data Augmentation 기법을 적용해 **공격 유형 간 데이터 불균형 문제를 해결**하고, Feature Engineering을 통해 **더 중요한 특징들을 선별**하고 새로운 특징을 추가해 **모델 성능을 개선**해보고 싶습니다.

임건형(3학년 팀) > 현재는 XSS 중심으로 설계했는데, 다음 단계에서는 **CSRF, SQLi, LFI 같은 다른 취약점 유형까지 범위를 넓히는 것**이 목표입니다. 또한 정적 분석(휴리스틱/흐름 분석) 쪽을 더 탄탄하게 만들어, LLM은 정말 애매한 케이스나 최종 판단/설명에 집중시키는 식으로 하이브리드 구조를 더 다듬고 싶습니다. PoC 검증도 더 체계화해서, 단순 탐지 결과가 아니라 실제 재현 가능성까지 지표로 보여주는 방향도 고민하고 있습니다.

권희진 (4학년 팀) > 향후에는 **접근성 측면에서의 사용자 부담을 더 줄이는 방향**으로 설계를 개선하고 싶습니다. 또한, 본 CAPTCHA를 학습한 적응형 Solver를 가정한 공격 실험을 통해 실제 방어 강건성을 정량적으로 평가하는 연구로 확장하고자 합니다. 최종적으로 CAPTCHA 단독이 아니라, 행동 기반 탐지와 결합된 다층 방어 구조로 발전시키는 것이 목표입니다.

Q. 프로젝트를 수행하는 과정에서 가장 어려웠던 점과 이를 어떻게 해결했는지 공유해주실 수 있을까요?

최장우 (1학년 팀) > 프로젝트를 수행하며 가장 어려웠던 점은 제한된 시간 안에 시도해볼 수 있는 선택지가 너무 많았다는 점이었습니다. 이를 해결하기 위해 모든 가능성을 다 시도하기보다는, 현실적으로 결과를 낼 수 있는 부분에 집중하도록 우선순위를 명확히 정했고, 작은 테스트베드를 먼저 만들어 아이디어를 빠르게 검증하는 방식으로 시행착오를 줄였습니다.

조준하 (2학년 팀) > 가장 어려웠던 점은 악성 문서 데이터를 수집하고 안전하게 분석하는 것이었습니다. 실제 악성코드를 다루는 만큼 호스트 시스템이 감염될 위험이 있어서, VMware 기반 샌드박스 환경을 구축해 격리된 환경에서 분석을 진행했습니다. 또한 176개의 feature를 정의하고 자동으로 추출하는 스크립트를 작성하는 과정도 쉽지 않았습니다. olevba 도구의 문서를 꼼꼼히 읽고, 기존 연구 논문들을 참고하면서 악성 문서에서 자주 나타나는 키워드와 패턴들을 정리했습니다. 팀원과 역할을 분담해 데이터 수집, feature 추출, 모델 학습을 병렬로 진행하면서 효율적으로 문제를 해결할 수 있었습니다.

임건형(3학년 팀) > 가장 어려웠던 점은 결과의 신뢰성을 확보하는 부분이었습니다. 오픈소스 플러그인을 대량으로 가져와 분석하다 보면, LLM의 결과가 매번 조금씩 흔들릴 수 있기 때문입니다. 그래서 결과 출력은 JSON 스키마로 고정해 일관성을 높이려고 했고, 팀원들이 다양한 테스트 케이스를 계속 던져 주면서 함께 튜닝해 나가는 방식으로 개선해 왔습니다. 앞으로도 이 과정을 반복하면서 더 안정적으로 발전시킬 계획입니다.

권희진 (4학년 팀) > 가장 어려웠던 점은 사람에게는 읽히되, OCR에게는 읽히지 않게 만드는 균형을 맞추는 것이었습니다. 이를 해결하기 위해 단순히 결과만 보는 것이 아니라, OCR이 실제로 어떤 단계에서 실패하는지를 로그와 출력 결과를 통해 반복적으로 분석했습니다. 이 과정에서 Solver의 전처리와 분할, 특징 추출 단계 각각을 분해해 바라보는 시각을 갖게 되었고, 설계 방향을 점진적으로 조정할 수 있었습니다.

Q. 프로젝트를 수행하는 과정에서 가장 어려웠던 점과 이를 어떻게 해결했는지 공유해주실 수 있을까요?

최장우 (1학년 팀) > 마지막으로 AI 및 보안 분야의 연구나 학술제 참가를 고민하는 후배 학우들에게는, 처음부터 완전히 새로운 것을 만들려 하기보다는 **이미 존재하는 기술과 도구를 깊이 이해하고 조합해보는 경험**이 중요하다고 말씀드리고 싶습니다. 직접 실험하고 실패해보는 과정이 가장 큰 자산이 되며, 의문이 생겼을 때 직접 만들어보고 검증해보는 태도를 계속 유지하셨으면 합니다.

조준하 (2학년 팀) > 학술제 준비 과정에서 논문을 읽고, 데이터를 직접 다루고, 모델을 학습시키면서 연구 역량이 많이 성장했습니다. 특히 예상했던 결과가 나오지 않았을 때 원인을 분석하고 해결하는 과정에서 문제 해결 능력을 키울 수 있었습니다. 이러한 과정에서 얻어갈 수 있는 점이 많으니, **관심 있는 주제가 있다면 부담 갖지 말고 도전**해보시길 추천드립니다.

임건형(3학년 팀) > 너무 완벽한 결과나 큰 성과를 준비해야 한다고 부담 갖기보다는, 진행 중인 프로젝트가 있거나 관심 있는 연구 주제가 있다면 일단 도전해 보시는 걸 추천드립니다. 준비하는 과정에서 배우는 게 정말 많고, 그 자체가 큰 경험이 되기 때문입니다. 또한 다른 학우들이 참여한 포스터를 보러 오기만 해도 다양한 인사이트를 얻을 수 있다고 생각해서, **부담 없이 참여**해 보셨으면 좋겠습니다.

권희진 (4학년 팀) > 처음부터 완성된 아이디어를 가지려고 하기보다는, 이미 존재하는 기술이 어떻게 공격받고 있는지를 먼저 이해해보는 것이 중요하다고 생각합니다. 보안 연구는 새로운 것을 만드는 것만큼, 기존 시스템의 가정을 의심해보는 과정에서 많은 아이디어가 나옵니다.
작은 문제의식이라도 직접 실험해보고 검증해보는 경험이 결국 가장 큰 자산이 되는 것 같습니다.
또한 다른 도메인의 지식을 이용해 아이디어를 발전시킨다면 더 창의적이고 새로운 결과물이 나오니 다른 **도메인의 지식을 참고하는 것**에 적극적이 되어 보시길 추천합니다!

취재 : 뉴스레터 6기 김주빈('23)

안티멀웨어 구조와 원리

전공 교과목을 추천받다

안티멀웨어 구조와 원리 과목은 악성코드 분석부터 탐지 기술 구현까지,
'안티멀웨어 소프트웨어의 핵심 원리를 폭넓게 다루는 전공 과목이다.

학생들은 악성코드 분석 방법론을 익히고, 그 분석 결과를 바탕으로 탐지 엔진 구조 설계와 탐지 룰(rule) 작성 과정을 학습한다. 강의는 이론과 실습을 겸하여 진행되며, 객체지향 C++로 구현된 간단한 탐지 시스템 예제 코드를 함께 분석하고 확장해 보는 프로젝트가 포함된다.

모든 실습 코드는 C++ 기반으로 작성되며, 표준 템플릿 라이브러리(STL)의 활용을 통해 효율적인 프로그래밍 기법도 익힌다. 이러한 실습 중심 접근을 통해 학생들은 실제 동작하는 안티멀웨어 시스템을 다뤄 보며 원리를 체득하게 된다.

주요 학습 내용

1. 악성코드 분석 기법
악성 코드 샘플에 대한 정적 분석을 수행하여 실행 파일 구조와 동작 특성을 파악한다
(예: Windows PE 파일 구조 분석 등).

2. 탐지 패턴 및 룰 설계
분석 결과 추출된 특징을 활용해 탐지 패턴 DB를 만들고 탐지 규칙을 설계한다. 예를 들어 대량의 악성코드 해시를 블룸 필터와 해시 테이블로 관리하여 탐지 성능을 높이고, 악성 파일 식별을 위해 탐지명 등의 정보를 연계 저장하는 방법을 실습한다.

3. 안티멀웨어 엔진 구조 분석
스캔 엔진, 패턴 DB, 실시간 감시 모듈 등 안티멀웨어 엔진을 구성하는 모듈별 설계 원리를 학습한다. 객체지향적 설계를 강조하여, 모듈별 책임 분리와 명확한 인터페이스 구현을 살펴본다. 예를 들어 파일 감시 기능은 추상 기반 클래스인 Watcher를 상속한 FileWatcher 클래스로 구현되어 모듈별 역할이 구분된다.

3. 실시간 감시 기능 구현
운영 체제의 파일, 프로세스, 레지스트리 이벤트를 후킹(hooking)하거나 감시하여 새로운 파일 생성이나 프로세스 실행 등 실시간 변화에 대응하는 방법을 다룬다. 사용자 모드에서 동작하는 감시 프로그램을 통해, 멀티스레드 기반으로 이벤트를 모니터링하고 탐지 엔진과 연동하는 과정을 실습한다. 이를 통해 동기화 기법(mutex 락 등)과 이벤트 처리 디자인 패턴의 활용도 경험한다.

진로 연계성

이 과목에서 다루는 내용은 **보안 소프트웨어 개발 분야로의 진로에 직접적인 밑거름**이 된다.
실제 백신 프로그램의 동작 원리와 유사한 시스템을 구축하고 분석해 봄으로써, 보안 제품 개발 직무에 필요한 코드 이해력과 시스템 설계 감각을 키울 수 있다.

예를 들어 향후 백신 엔진 개발이나 엔드포인트 위협 탐지 시스템 구현 직무를 맡게 될 경우,
본 과목에서 다진 객체지향 설계 역량과 악성코드 탐지 기술에 대한 이해가 큰 도움이 될 것이다.

취재 : 뉴스레터 6기 이창민('21)

고려대학교
세종SW중심대학사업단 인터뷰

Q. 먼저 고려대학교 세종SW중심대학사업단에 대한 간단한 소개와 교수님께서 담당하고 계신 주요 업무를 소개해 주실 수 있을까요?

A, 안녕하세요, **고려대학교 세종SW중심대학사업단에서 교육과정 개발 등 실무총괄**을 맡고 있는 **연구교수 권현지**입니다.

저희 사업단은 국가 디지털 혁신을 주도할 SW·AI 융합 교육 선도 대학으로 비전을 수립하고 국가와 산업 수요에 맞춘 실무형 글로벌 SW·AI 인재 양성과 SW·AI 가치를 확산하여 행정복합도시 디지털 혁신을 견인하기 위한 사업을 추진하고 있습니다.

Q. 정부의 'SW중심대학' 사업의 전반적인 취지와 목표가 무엇인지, 그리고 고려대학교 세종캠퍼스가 이 사업에서 어떤 역할을 수행하고 있는지 설명해 주신다면요?

A, **SW중심대학 사업**은 과학기술정보통신부가 2015년부터 **SW·AI 중심 대학 개편과 인재 양성을 위해 추진한 사업**입니다. 현재 국내 58개 대학이 참여하고 있습니다.

특히 고려대학교 세종캠퍼스가 행정수도에 위치한 만큼, 저희 사업단은 행정수도부터 국가 전반에 이르기까지 국가 디지털 혁신을 견인하고자 노력하고 있습니다. 구체적으로, 교내에서는 SW·AI 기초·융합·전공교육, 산학협력을 고도화하여 국가 발전에 주도적으로 기여할 수 있는 인재를 양성하고 있으며 동시에 SW·AI 가치를 국가와 지역에 확산하기 위해 힘쓰고 있습니다.

Q. 세종 SW중심대학사업단에서 운영 중인 여러 프로그램 가운데, 인공지능사이버보안학과 학생들이 특히 주목하면 좋을 핵심 사업을 두 세 가지 정도 소개해 주실 수 있을까요?

1. 크림슨SW마일리지 장학 제도

크림슨SW마일리지는 **SW·AI 관련 활동**을 하여 **마일리지 점수**를 쌓고 그 **점수를 학기 말에 장학금으로 바꿀 수 있는 제도**입니다. 비교과·융합전공 · KTX 마이크로디그리 등 사업단이 공지한 프로그램에 참여하면 마일리지가 적립됩니다.

▲ 소개 QR

장학금 신청은 **마일리지 50점 이상부터 신청 가능**하며 **1점당 1만 원으로 환산**됩니다. SW학과는 학기당 최대 200만 원, 비SW학과는 최대 150만 원까지 장학금을 받을 수 있습니다. 마일리지는 해외 인턴십·해외 연수 프로그램 서류 평가에도 반영됩니다.

2. KTX 마이크로디그리

KTX(KUS emerging Technologies eXperience) 마이크로디그리는 **SW·AI 핵심 기술 관련 과목을 최소 12학점 이수**하며 **해당 전문지식과 실무 역량을 KTX처럼 빠르고 효과적으로 함양**하고 이를 **공식적으로 인정받는 제도**입니다. 이수 완료 시 크림슨SW마일리지 60점이 제공되며 신청자에 한하여 고려대학교 교무처장 명의로 이수증이 발급됩니다.

▲ 소개 QR

2025년 12월 기준, KTX 마이크로디그리 종류는 총 5가지로 인공지능 마이크로디그리, 클라우드 마이크로디그리, 빅데이터 마이크로디그리, 블록체인 마이크로디그리, 사이버보안 마이크로디그리로 구성됩니다.

3. 글로벌 대학·기업 연수 프로그램

글로벌 연수 프로그램은 **해외 대학·연구소·기업을 방문**해 **최신 SW·AI 기술과 산업 현장을 경험하는 프로그램**입니다. 매년 1회 이상 운영하여 SW·AI 현장 연구·산업 적용·스타트업 생태계를 체험하고 국제 협력 네트워크와 진로 확장 기회를 제공하는 것이 목표입니다. 참여 혜택으로는 해외 프로젝트·해외 인턴십 연계 가능성 탐색, 현업 관계자 멘토링 기회 확보 등이 있습니다. 본 프로그램의 참여 인원 선발 평가 기준에는 크림슨SW마일리지 점수가 반영되니 참고 바랍니다.

▲ 2025년도 크림슨SW아카데미

▲ 2025년도 SW인재페스티벌 '인기상' 수상

Q. 각종 프로그램 신청이나 서류 작성, 선발 과정에서 학생들이 자주 어려움을 겪거나 실수하는 부분이 있다면, 이를 줄이기 위한 조언이나 행정적인 '팁'을 알려주실 수 있을까요?

A, 학생들이 가장 자주 겪는 어려움은 **프로그램 신청 시기를 놓치거나 제출해야 할 서류를 누락**하는 부분입니다. 특히 선착순으로 빠르게 마감되는 프로그램은 준비가 조금만 늦어져도 기회를 놓치는 경우가 자주 발생합니다.

프로그램의 신청 기간과 제출 서류 조건 등을 미리 꼼꼼히 확인하고, 사업단 홈페이지와 인스타그램 계정을 자주 확인하는 작은 습관이 여러 기회를 확보하는 데 큰 도움이 될 것입니다.

▲ 고려대학교 세종SW중심대학사업단 공지사항

▲ 고려대학교 세종SW중심대학사업단 인스타그램

Q. 사업단 관점에서 볼 때, 인사보 학생들이 사업단 프로그램을 활용해 특히 강화했으면 하는 역량이나 역할은 무엇이라고 생각하시나요?

A, 사업단은 인공지능사이버보안학과 학생들이 **AI 기반 보안 문제 해결 역량과 융합적 사고·협업 능력을 집중적으로 강화**하길 기대하고 있습니다. 미래 보안 전문가는 기술 지식을 넘어 실제 데이터를 활용해 위협을 분석하고 대응할 수 있어야 하며, 다양한 산업·도메인과 연계해 문제를 종합적으로 해결할 수 있는 역량이 요구됩니다.

이에 사업단은 **기업연계형 캡스톤디자인, 산학협력 프로젝트 등 실전 중심 프로그램**으로 인공지능사이버보안학과 학생들이 AI 기반 보안 전문성과 실전 경험을 갖춘 핵심 인재로 성장할 수 있도록 지속적으로 지원하고자 합니다.

Q. 1 · 2학년 인사보 학생들이 비교적 이른 시기부터 준비해 두면, 3 · 4학년이나 졸업 이후에 큰 도움이 될 만한 경험이나 준비 요소-가 있다면 어떤 것들을 추천하고 싶으신가요?

A, 1 · 2학년 시기는 **자신의 진로 방향을 탐색하고 목표를 세우는 데 중요한 시기**입니다. 특히 기초 역량을 쌓아가며 진로를 탐색할 수 있는 다양한 경험 속에서 '나는 특히 어떤 문제에 관심과 흥미가 있고 무엇에 의미를 느끼는 사람인가'를 알아가는 과정이 중요합니다.

이를 위해 **전공 지식 기초**를 다지면서 동시에 **관심있는 진로 분야에 관한 다양한 상호작용을 경험**하는 것이 필요합니다. 예를 들면 학과 선배·산업계 멘토·교수님과의 대화, 교내·외 프로젝트나 학습 커뮤니티 활동, 봉사활동 참여 등을 통해 직·간접적인 경험을 쌓아보는 것이 효과적입니다.

본 사업단에서는 이 과정을 돕기 위해 연말에 'AI와 함께하는 진로여행 워크북'을 전자책으로 제공하여 여러분이 진로 목표를 구체화하고 성장의 방향을 설정할 수 있도록 지원하고자 합니다.

Q. 앞으로 3~5년 안에 세종 SW중심대학사업단이 꼭 이루고 싶은 목표나, '이건 우리만의 색깔로 만들고 싶다'고 생각하는 대표 브랜드·프로그램이 있다면 무엇인가요?

A, 첫째, SW·AI 기초·융합교육 측면에서 예비 입학생과 전교생의 **SW·AI 기초교육을 강화하기 위한 교과목을 신설**하고 X+SW·AI, SW·AI+X **융합 전공을 확대**하여 학**내의 실질적 SW·AI 융합**을 이루고 싶습니다.

둘째, SW·AI 전공교육과 SW·AI 산학협력 강화를 위해서 **기업 주도형 교육 혁신을 위해 다양한 산학연계 프로그램을 운영**하여 **실제 산업 현장의 문제를 해결하는 교육 생태계를 구축**하고자 합니다.

셋째, SW·AI 가치를 지역과 국가에 확산하기 위해 지속적으로 정부부처와 공공기관 공직자, 초·중·고 학생과 일반시민을 위한 **SW·AI 리터러시 향상을 위한 교육을 실행할 예정**입니다.

이 외에도 글로벌 대학·기업 연수 프로그램, 교내외 SW·AI·창업 경진대회 운영, 실습실 및 온·오프라인 교육 환경 개선, 그리고 SW·AI 기자재 확충 등으로 학습 몰입도와 교육 실효성을 꾸준히 높여나가는 것이 본 사업단이 꼭 이루고 싶은 목표입니다.

Q. 끝으로, 세종 SW중심대학사업단에 관심이 있는 인공지능사이버보안학과 학생들과 인사보 뉴스레터 독자들에게 전하고 싶으신 말씀이 있다면 자유롭게 부탁드립니다

A, 마지막으로 전하고 싶은 말은 **SW·AI 기술**은 **여러분이 상상하는 것을 현실로 만드는 강력한 실행 도구가 될 수 있다는 점**입니다. 아직 진로가 아직 명확하지 않아도 괜찮습니다. 중요한 것은 '내가 궁금한 것이 무엇인지 성찰하고, 작게라도 직접 실행 보는 용기'입니다. 작은 호기심을 프로젝트로, 비교과 활동으로, 코드 한 줄 연습으로 실천해 보는 경험이 중요합니다.

앞으로는 **호기심을 행동으로 옮길 수 있는 사람**이 큰 경쟁력을 가지게 될 것이라고 봅니다. 그 과정에서 SW·AI 기술은 여러분의 아이디어를 실제로 구현해줄 든든한 도구가 될 것입니다. 이와 더불어 세종SW중심대학사업단은 **여러분이 생각한 것을 실행할 수 있는 기회와 환경을 제공하는 파트너**가 되겠습니다.

언제든 문을 두드려 주세요. 여러분의 도전과 성장을 진심으로 응원합니다.

취재 : 뉴스레터 6기 고건우('25)

올해의 보안 이슈

SK텔레콤 유심 정보 유출, BPFDoor가 드러낸 통신 인프라 보안의 민낯

2025년 4월 18일, SK텔레콤 홈가입자서버(HSS)에서 가입자 유심(USIM) 정보가 외부로 전송된 사실이 확인되며 국내 통신 인프라의 근본적인 보안 수준을 다시 묻게 하는 사건이 발생했다.

민관합동조사단 최종 결과에 따르면 유출 규모는 약 9.82GB, 가입자 식별번호(IMSI) 기준 약 2,696만 건에 달하며, 전화번호와 IMSI뿐 아니라 유심 인증 키(Ki, OPc)를 포함한 유심 관련 정보 25종이 포함된 것으로 밝혀졌다.

이러한 정보는 이동통신망에서 가입자를 식별하고 인증하는 핵심 비밀값으로, 이후 2차 공격과 계정 탈취에 활용될 수 있다는 점에서 단순한 개인정보 유출을 넘어선 심각한 보안 사고로 평가된다. 개인정보보호위원회는 계정 관리 부실과 암호화 미흡 등을 이유로 SK텔레콤에 약 1,348억 원 규모의 과징금을 부과하며 역대 최대 수준의 제재를 결정했다.

BPFDoor 계열 악성코드, BPF를 악용한 리눅스 장기 잠복형 백도어

이번 침해사고의 핵심 도구로 지목된 것은 리눅스 기반 백도어인 **BPFDoor 계열 악성코드**이다.
민관합동조사단은 SK텔레콤 리눅스 서버 수만 대를 전수 조사한 결과, 감염 서버에서 BPFDoor 계열 악성코드 수십 종과 웹쉘 등이 함께 발견되었음을 공개했다.

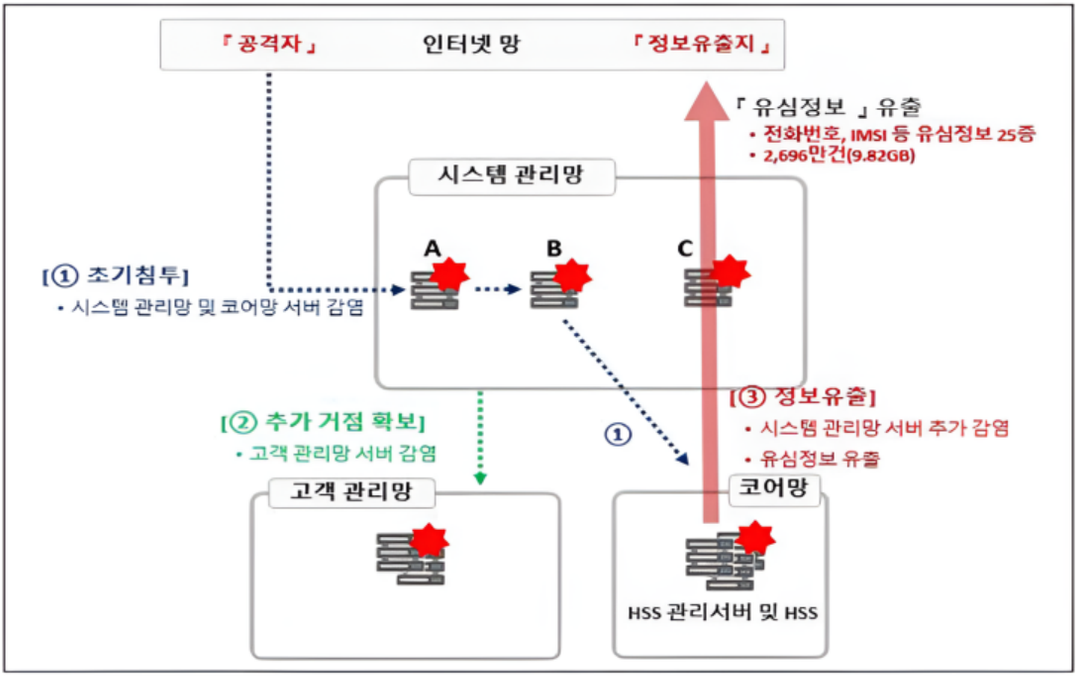
BPFDoor는 Berkeley Packet Filter(BPF)를 이용해 커널 레벨에서 네트워크 패킷을 감시하며, 특정 바이트 시퀀스를 포함한 이른바 매직 패킷이 도착했을 때만 백도어 기능을 활성화하도록 설계된 것이 특징이다. 이 과정에서 별도의 리스닝 포트를 열지 않고도 특정 패킷을 수신할 때 실행되는 패킷 처리 루틴을 후킹해 리버스 쉘이나 포트 포워딩을 수행하며, 이를 통해 내부망에 재진입할 수 있는 통로를 은밀하게 유지한다.

프로세스 이름을 정상 데몬처럼 위장하고 로그 기록을 최소화하는 등 은닉 기능도 갖추고 있어, 탐지 장비가 부족하거나 모니터링 체계가 미흡한 환경에서는 수년간 잠복이 가능한 구조로 평가된다.

외부와 맞닿은 시스템 관리망 서버 A, 초기 침투의 관문으로 전락

조사 결과에 따르면 공격의 출발점은 인터넷과 연결된 시스템 관리망 내 특정 리눅스 서버, 이른바 서버 A였다. 2021년경 공격자는 이 서버의 취약점을 악용하거나 계정 탈취를 통해 최초 접근에 성공한 뒤, CrossC2와 같은 원격 제어 악성코드를 설치해 장기 거점을 확보한 것으로 파악된다.
문제는 이 서버에 **동일 관리망 내 다른 서버들의 계정 ID와 비밀번호가 평문으로 저장**되어 있었다는 점이다.

이로 인해 공격자는 추가적인 브루트포싱이나 취약점 공격 없이도 **저장된 계정 정보를 재사용하는 방식**으로 내부 이동을 이어갈 수 있었고, **시스템 관리망 전체**가 사실상 **하나의 로그인 정보 저장소에 종속된 구조**였다는 사실이 드러났다.



서버 B와 HSS 관리서버, 평문 계정정보를 딛고 코어망으로 확장

서버 A에서 확보한 계정 정보를 활용해 공격자는 같은 관리망의 또 다른 서버인 B로 이동했다.
이 서버에는 코어망 음성통화인증(HSS) 관리서버의 로그인 ID와 비밀번호가 마찬가지로 평문으로 저장되어 있었으며, 조사단은 공격자가 이 정보를 이용해 2021년 말에 HSS 관리서버와 HSS 서버들에 순차적으로 접속한 것으로 결론 내렸다.

이 과정에서 **BPFDoor 계열 악성코드가 HSS 구간에 설치**되어 **코어망 내부에 은밀한 재접속 통로**가 만들어졌고, 이후 수년간 통신 인프라의 심장부에 해당하는 **가입자 인증 영역이 외부 위협에 노출**된 상태로 유지되었다.

계정 권한 구조 상 코어망 접근 권한을 가진 자격증명이 보안 수준이 낮은 관리망 서버에 그대로 저장되어 있었던 점은, **논리적 망 분리가 계정 관리 미흡으로 쉽게 무력화될 수 있음**을 보여준다.

고객 관리망과 유심 정보 유출, 2025년 4월 18일 최종 단계로 이어진 침해

초기 침투 이후 공격자는 2022년 무렵 고객 관리망과 통합고객인증시스템(ICAS)으로 거점을 확장하며 웹쉘과 추가 백도어를 심어 두었고, 일부 서버에서는 이름과 생년월일, 주소, 단말기 식별번호(IMEI)와 같은 정보가 평문으로 저장되어 있었음이 조사 과정에서 확인되었다.

다만 이 구간의 **로그 보관 기간이 짧아 실제 유출 여부를 끝까지 입증하지는 못했다는 한계**도 함께 드러났다.
최종적으로 2025년 4월 18일, 공격자는 이미 설치해 둔 악성코드와 자격증명을 활용해 HSS 서버 세 대에서 유심 관련 데이터를 조회·추출한 뒤, 압축 파일 형태로 외부의 중간 서버를 경유해 반출한 것으로 조사되었다.
이때 유출된 정보에는 휴대전화번호, IMSI, 유심 인증 키(Ki, OPc), 내부 관리용 코드 등 총 25종의 항목이 포함되어 있었고, SK텔레콤은 이후 공지를 통해 고객 대상 유출 사실과 범위를 공식 안내했다.

계정 관리 부실과 망 분리 실패, 고급 악성코드보다 더 치명적인 구조적 취약점

민관합동조사단은 최종 보고서에서 이번 사고의 핵심 원인으로 **계정 정보 관리 부실, 망 분리 및 접근통제 실패, 주요 정보의 암호화 조치 미흡, 보안 패치와 백신 적용 지연**을 함께 지적했다.
음성통화인증 관리서버의 계정정보가 다른 서버에 평문으로 저장된 상태였고, 시스템 관리망 내 서버들의 비밀번호가 장기간 변경되지 않았으며, 코어망과 관리망 사이의 연결 구조도 최소 권한 원칙과 거리가 먼 설계였다는 점이 공식 문서에서 반복적으로 언급된다.

여기에 더해, 수년 전 공개된 리눅스 커널 취약점과 구버전 OS를 장기간 패치 없이 유지하고, 일부 서버에는 백신조차 설치하지 않았던 운영 관행도 총체적 보안 수준 저하의 배경으로 지적된다.
결과적으로 BPFDoor라는 고급 백도어의 존재 자체보다, 이런 기본 보안 통제의 붕괴가 공격자가 4년간 인프라 내부에 머무르며 최종적으로 대규모 유출을 실현할 수 있게 만든 토대가 되었다.

고급 공격 기법보다 치명적이었던 패치·계정·로그 관리 실패

SK텔레콤 유심 정보 유출 사건은 통신 인프라를 노린 첨단 악성코드 사용 사례인 동시에, 패치 관리, 자격증명 관리, 네트워크 분리, 로그 보존과 같은 기본 보안 원칙이 현장에서 어떻게 무너지는지 보여주는 실증 사례로 남는다.

BPFDoor는 **BPF를 활용해 커널 레벨에서 패킷을 필터링**하고 **매직 패킷을 통해 은밀하게 재접속 통로를 유지**하는 등 현대 리눅스 환경에서 주목해야 할 공격 기법을 집약한 백도어이지만, 이번 사건의 피해 규모와 장기 잠복을 가능하게 만든 요인은 허술한 계정 관리와 취약한 시스템 구성, 불충분한 모니터링과 로그 보존이었다.

이 사례는 **실제 인프라 운영 환경에서 이론과 규정이 어떤 지점에서 실패할 수 있는지** 구체적인 맥락을 제공한다.

취재 : 뉴스레터 6기 이창민('21)

편찬위원

위원장 배은서 (인공지능사이버보안학과 23학번)

위원 이창민 (인공지능사이버보안학과 20학번)
김주빈 (인공지능사이버보안학과 23학번)
심재규 (인공지능사이버보안학과 24학번)
양희지 (인공지능사이버보안학과 24학번)
고건우 (인공지능사이버보안학과 25학번)

집필분담

이창민('20)
학과 전공 과목 추천
올해 보안 이슈

김주빈('23)
한미란 학과장님 인터뷰
학술제 수상자 인터뷰

심재규('24)
2학기 개강총회
새 학생회장 인터뷰

고건우('25)
구자훈 교수님 인터뷰
세종 SW중심대학사업

발행일 2025년 12월 21일

편집인 배은서('23), 양희지('24)

감수위원 김희석 교수님

발행처 인공지능사이버보안학과 뉴스레터 편집 위원회