스마트
보안
학부

KOREA UNIVERSITY
고려대학교 인재 양성·진로 가이드북

Since 2021

스마트시대의 IT기술을 겸비한
보안 인재를 양성하는

스마트 보안 학부

Division of Smart Security

스마트보안학부는 스마트 시대의 핵심인 소프트웨어와 사이버보안, 그리고 인공지능과 같은 신기술 분야에서 국내 최고의 교수진을 중심으로 구성되어 2021학년 신설된 학부입니다. 본 학부는 학계, 산업계, 법조계, 정부 기관, 대기업 등에서 요구하는 '스마트시대에 사이버보안을 적용, 응용 및 연구하고 소프트웨어, 인공지능 기본기를 갖춘 엔지니어와 학자'를 양성합니다.

http://scs.korea.ac.kr

인재발굴처
홈페이지
바로가기

딱!

이런 학생 스마트보안학부에

- 소프트웨어, 인공지능 기본기를 갖춘 스마트 사회의 핵심 엔지니어나 학자가 되고 싶다.
- 스마트시대에 사이버보안을 적용, 응용 및 연구하고 싶다.
- 국가나 대형 범죄 집단이 주도하는 고도의 해킹 위협(State-Sponsored Hacking)에 대한 전문가가 되고 싶다.

스마트 보안 학부?

지금 세계는 AI(Artificial Intelligence)의 급속한 발전으로 인해 산업과 사회(삶) 전반에 걸친 거대한 문명사적 변화를 맞이하는 중입니다. 이제는 AI가 인간의 지적 기능도 수행하는 수준까지 발전함에 따라, AI는 이제 산업과 사회 모든 영역에 걸친 패러다임 변화를 촉발할 것입니다. 향후 AI는 그 자체로 막대한 부가가치를 창출하는 산업인 동시에 산업의 근본적 혁신을 가져오며, 일자리 변동 등 사회의 변화도 유발할 것입니다.
최근 고용정보원은 인공지능(AI)이나 로봇으로 대체가 쉬운 직업과 대체가 어려운 직업을 발표한 결과에 따르면 사이버보안(Cyber Security) 전문가의 경우 대체가 어려운 직업군으로 분류되어 있으며, 대체 비율은 0.338으로 이는 사이버보안과 관련한 분야들 중에 34%만이 AI로 대체 가능하며, 66%는 고도의 창의성이 요구돼 AI로 대체하는 것이 불가능하다는 것을 의미합니다. 이러한 이유로 미국 등 선진국의 경우, AI Security와 Human Security를 조합해 각종 사이버 위협에 대응하려는 계획을 추진하고 있습니다. 고려대학교 스마트보안학부는 일상적 사이버 위협에 신속히 대응하는 것을 목표로 차세대 AI Security 개발 인력 양성에 초점을 맞추고 있습니다.

인공지능시대의 IT기술을 겸비한 사이버보안 인재의 요람

스마트 보안학부의 엔진

스마트보안학부는 정보보호대학원의 20여 년의 교육 및 연구 경험과 사이버국방학과의 10여 년의 운영 경험을 토대로 중견 학부 같은 교육프로그램과 연구프로그램, 산학협력 프로그램을 운영하고 있습니다.
이를 통해 세계적 수준의 사이버보안 인재 육성기관으로 발돋움하고 있습니다.

전공 수업

전공수업은 소프트웨어 기본, 사이버 보안 기본, 응용 및 리더십의 네 가지 주요 영역을 다룹니다.

전공수업은 융합되어 활용됩니다. 인공지능 보안과 같은 새로운 분야도 전공수업에서 배울 수 있으며 이를 위해서는 인공지능 개념과 사이버보안 개념을 학습해야 합니다.

학생이 자신의 관심 분야를 선택하여 공부할 수 있으며, 또한 사회의 요구에 따라 지속해서 새롭게 과목을 발전시키고 있습니다.

특별 프로그램

마이크로디그리(최소 12학점 이수)

① 암호기술(Cryptographic Technology) 암호기술은 수학과 컴퓨터 과학을 접목한 학문입니다. 본 과정은 암호기술을 이해하기 위한 수학, 암호기술을 습득하고, 이를 응용 할 수 있는 능력과 암호기술을 구현하여 다양한 분야에 활용할 수 있는 것을 목표로 합니다.
편성:암호수학, 암호구현및실습, 암호프로토콜, 현대암호학응용, 스마트보안응용, 캡스톤디자인 I

② 인공지능보안(AI Security) 인공지능의 수학적 구조에 대한 이해를 바탕으로 인공지능 보안 기술을 이해하고 신뢰가능한 인공지능 개발과 다양한 인공지능 보안 응용의 이해를 목표로 합니다.
편성: 스마트보안수학, 인공지능보안수학, 인공지능보안 I·II, 캡스톤디자인 I

개인정보보호융합전공

실무역량을 갖춘 개인정보보호 활용 전문인력 양성을 목표로 합니다. 스마트보안학부 주도하에 개인정보보호 기술·정책 융합교육을 실시할 수 있도록 법학전문대학원 및 행정학과가 협력하여 2023년 2학기에 신설됩니다.

학과목에 대하여

소프트웨어 및 보안 기본 — 스마트보안수학, 인공지능보안수학, 암호수학, 정형기법, 컴퓨터네트워크, 인공지능보안 I·II, 데이터보안 운영체계 등

사이버보안 — 스마트보안개론, 현대암호학, 암호프로토콜, 해킹개론, 하드웨어보안, 역공학, 위험관리, 디지털포렌식 등

사이버보안 응용 — 디지털포렌식개론, 시큐어코딩, 데이터보안, 시큐어소프트웨어공학 I·II, 소프트웨어보안, 스마트보안응용, 빅데이터응용보안 등

리더십 — 사이버윤리, 사이버기술과법, 개인정보보호, 스타트업창업방법론, 캡스톤디자인 I·II, 현장실습 I·II·III 등

스마트 보안학부의 어제와 오늘

2000년에 고려대학교에서는 정보보호대학원을 설립하여 석박사 전문인력양성을 시작하였습니다. 2021년에는 이러한 경험을 바탕으로 스마트보안학부가 설립되어 사이버보안 기술을 기초부터 익힌 사이버보안 기술이 내재화된 인재 양성을 시작했습니다. 사이버 위협은 점점 더 정교해지고 있으며, 사이버 범죄자들은 취약점을 악용하기 위한 새로운 방법을 끊임없이 개발하고 있습니다. 스마트보안학부는 이러한 사회에 사이버보안을 이끌 인재를 육성할 요람이 될 것입니다.

스마트 보안학부의 미래

사이버 보안의 미래는 흥미진진하면서도 매우 도전적입니다. AI와 같은 새로운 기술의 탄생은 새로운 보안 기술을 필요로 하게 되며, 점점 더 많은 시스템이 인터넷에 연결됨에 따라 사이버 범죄자의 공격할 수 있는 방법은 계속 증가하고 있습니다. 우리 학부에서는 미래 사회를 안전하게 지키는 상상할 수 없는 보안 기술의 전문가를 배출할 것입니다.

Blue Ocean

새로운 기술은 항상 사이버보안이 필요합니다. 인공지능은 인공지능 보안을, 자율자동차는 자율자동차 보안이 필요합니다. 사이버 보안 기술이 없으면 아무리 새로운 기술이라도 무용지물이 됩니다. 기술과 보안은 항상 함께합니다.

얘들아! 이것만은 명심하자

핵심 기술을 습득하세요. 사이버 보안 분야에서 일하기 위해 알아야 할 기본 과목들이 있습니다. 수학, 컴퓨터, 해킹 등 많이 배우시기 바랍니다.

실습 경험을 얻으세요. 사이버 보안 분야에서 일하는 방법을 가장 잘 배우는 방법은 경험을 쌓는 것입니다. 수업 외에도 동아리 활동, 해킹 대회, 사이버시큐리티 컨퍼런스 또는 인턴십과 같은 실습 경험을 제공하는 많은 리소스를 사용할 수 있습니다.

새로운 것을 계속 배우세요. 사이버 보안은 빠르게 발전하는 분야이므로 최신 기술을 따라잡기 위해 최선을 다하는 것이 중요합니다.

인내심을 가지세요. 사이버 보안 분야는 새로운 분야입니다. 포기하지 말고 계속 학습하고 경험을 쌓으시길 바랍니다.

관련 자격 및 시험

국내

정보처리기사, 정보보안기사/산업기사, 디지털포렌식전문가, CPPG(개인정보관리사), 산업보안관리사, 정보보호관리체계(ISMS)인증심사원

해외

CISSP(Certified Information Systems Security Professional), CCFP(Certified Cyber Forensics Professional),SSCP(Systems Security Certified Practitioner), CAP(Certified Authorization Professional),CSSLP(Certified Secure Software Lifecycle Professional), HCISPP(HealthCare Information Security and Privacy Practitioner), CCSP(Certified Cloud Security Professional),CISA(Certified Information Systems Auditor), CISM(Certified Information Security Manager),CGEIT(Certified in the Governance of Enterprise IT),CRISC(Certified in Risk and Information Systems Control),EnCE(EnCase Certified Examiner)

길을가는 후배에게

이렇게 다를 줄이야!
고교시절 생각했던 전공에 대한 오해

사이버보안의 기초와 핵심을 배우고, 실습해 봄으로써 항상 새로운 것을 꾸준히 배우세요. 그러면 사이버보안이라는 첨단분야에서 활동하는 후배님의 꿈을 이룰 것입니다. 우리가 도와 드리겠습니다.

알쏭달쏭 전공과목 (* 정보대학 컴퓨터학과 교과목)

1 학년

스마트보안개론, 스마트보안수학, C언어및실습, 계산논리

2 학년

암호구현 및 실습, 정형기법, 인공지능보안수학, 암호수학, 디지털포렌식개론, 현대암호학, 역공학, 해킹개론, 시큐어코딩, 사이버윤리, 컴퓨터구조*, 컴파일러* 논리설계*

3 학년

인공지능보안 I·II, 암호프로토콜, 컴퓨터시스템보안, 데이터보안, 위험관리, 컴퓨터네트워크보안, 현대암호학응용, 시큐어소프트웨어공학 I, 운영체제*, 컴퓨터네트워크*, 소프트웨어보안*

4 학년

시큐어소프트웨어공학 II, 빅데이터응용보안, 사이버기술과법, 개인정보보호, 캡스톤디자인 I·II, 디지털포렌식실무, 하드웨어보안, 스마트보안응용, 스타트업창업방법론, 현장실습 I·II·III 등

동아리 & 학회(학생 자치 활동)

KU WiCys
마이크로소프트가 전세계적으로 지원하는 여학생 정보보안 관련 동아리

MatKor
수학 이론 학습 및 적용을 통한 프로그래밍 및 문제 해결 능력 향상과 프로젝트를 통한 실무 능력 및 개발 능력 향상을 목적으로 하는 동아리

$clear
건강 증진 목적 동아리

졸업 후의 진로

산업계
구글, 아마존, 마이크로소프트, 애플, 페이스북, IBM, 네이버, 카카오, 삼성 등 보안 및 AI보안 관련 글로벌 대기업에 진출 가능

정부·공공기관·기타
국가정보원, 경찰, 행정기관 등으로 진출 가능

창업
스마트 사회에서 믿고 생활하는 데 핵심 요소인 사이버보안 관련 다양한 보안 관련 기업, 보안이 내재화된 소프트웨어기술 기반 기업

용어상식

소프트웨어 보안 (Software Security)

소프트웨어 보안은 소프트웨어를 보호하고, 외부에서의 공격과 악용을 방지하는 것을 의미합니다.
먼저, 소프트웨어 개발 초기부터 보안을 고려하여 보안을 내재화하면서 개발하는 것이 중요합니다. 이를 위해서는 보안 요구 사항을 분석하고, 시큐어 바이 디자인과 시큐어 코딩으로 취약점을 미리 파악하고 예방하여야 합니다.
소프트웨어 보안 방법에는 인증과 권한부여, 암호화, 취약점분석, 코드리뷰, 사이버시큐리티 윤리, 규정, 법 등이 있습니다.

네트워크 보안

네트워크 보안은 네트워크에 연결된 컴퓨터 및 디바이스에 대한 사이버 보안 보호를 말합니다. IT 팀은 방화벽 및 네트워크 액세스 제어와 같은 네트워크 보안 기술을 사용하여 사용자 액세스를 규제하고 특정 디지털 자산에 대한 권한을 관리합니다.

클라우드 보안

클라우드 보안은 클라우드에서 실행되는 데이터 및 애플리케이션을 보호하기 위해 조직에서 취하는 조치를 말합니다. 이는 확장 가능한 환경에서 고객 신뢰를 강화하고 운영의 내결함성을 보장하며 데이터 개인 정보 보호 규제를 준수하는 데 중요합니다.

AI 보안

chatGPT로 문을 연 인공지능시대는 인공지능 그 자체가 사회 모든 부분의 핵심요소가 되어 가고 있습니다. 이러한 이유로 인공지능에 대한 “회피공격”, “데이터오염공격” 등 다양한 악의적 공격이 예상되고 있으며, 이에 대한 사이버보안 기술이 필요하게 됩니다.

데이터 보안

데이터 보안은 강력한 스토리지 시스템과 보안 데이터 전송을 통해 전송 중 데이터와 저장 데이터를 보호합니다. 개발자들은 잠재적 데이터 침해로부터 운영 복원력을 유지하기 위해 암호화 및 격리된 백업과 같은 사전 예방적 조치를 사용합니다. 개발자는 일부 경우에 AWS Nitro System을 사용하여 스토리지 기밀성을 유지하고 운영자 액세스를 제한합니다.

제로 트러스트 (Zero Trust)

제로 트러스트(Zero Trust)는 전통적인 신뢰 기반 접근보다 검증과 제어를 중심으로 한 보안 접근 제어 철학입니다. 이 개념은 모든 사용자, 장치 및 리소스에 대해 신뢰를 전제로 하지 않고 항상 인증과 권한 검사를 수행하여 보안 위협을 최소화합니다. 제로 트러스트는 현대적인 IT 환경에서 더욱 중요해진 데이터 유출과 내부 침해 사고에 대응하기 위해 도입되었습니다. 이를 통해 기업은 보다 견고한 보안 체계를 구축하고, 데이터와 시스템을 효과적으로 보호할 수 있게 됩니다. 제로 트러스트는 신뢰를 기반으로 하는 보안 전략의 한계를 극복하고, 모든 접근 시도에 대해 미심쩍은 태도를 가지며 검증과 제어를 통해 더욱 안전한 환경을 조성하는 것을 목표로 합니다.

디지털 포렌식 (Digital Forensics)

디지털 포렌식은 디지털 증거물을 수집하고 분석하여 범죄 수사에 활용하는 과학수사 기술입니다. 디지털 포렌식은 디지털 기기에 남아있는 데이터를 복구하고 분석하여 범죄의 단서를 찾아냅니다. 범죄 수사와 사법 절차에 도움을 주는 핵심 기술이라고 할 수 있습니다.

침투 테스트 (Penetration Testing)

침투 테스트란 컴퓨터 시스템이나 네트워크의 보안 취약점을 찾아내기 위해 고의적으로 공격을 시도하는 테스트입니다. 이는 실제 공격자의 행동과 유사한 방식으로 시스템을 탐색하고, 보안 취약점을 식별하고 해결책을 찾는 데에 활용됩니다.
침투 테스트는 보안 전문가나 윤리적 해커들이 수행하는 작업으로, 시스템의 보안 수준을 향상시키기 위한 절차입니다.
침투 테스트의 방법과 도구에는 외부에서의 공격 시뮬레이션, 네트워크 스캐닝, 시스템 해킹 등을 포함할 수 있습니다. 주요 목표는 시스템의 취약점을 찾고, 데이터 유출, 시스템 마비 등과 같은 위험을 예방하는 것입니다.