2021 NetSec-KR

'K-사이버보안' 의 현재와 미래

The 27th
Network Security
Conference-Korea

제27회
정보통신망 정보보호
컨퍼런스

초청강연

Keynote 1

디지털 안심국가 실현을 위한 K-사이버방역 추진전략

홍진배 과학기술정보통신부/정보보호네트워크정책관

'디지털안심 국가'실현을 위한 'K-사이버방역 추진전략' 소개

- 디지털안심 국가 기반 구축
- 보안 패러다임 변화 대응 강화
- 정보보호산업 육성 기반 확충 등 3대 중점전략

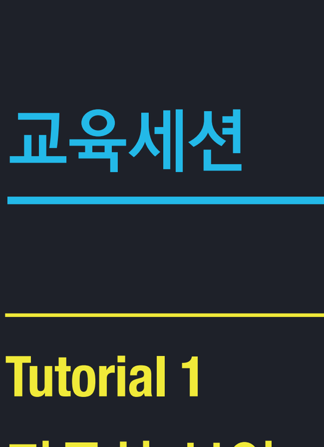
보안 패러다임 변화에 대응하기 위한 기술개발(R&D) 추진 방향

- 비대면·디지털전환 특성을 고려한 핵심 보안기술 확보
- 차세대 융합보안 전략 기술 확보
- 사이버 범죄 예방 등 사회안전망 확보 보안

정보보호산업 기반 확충을 위한 정보보호 인력양성 방안

- 산업계 수요 기반 정보보호 신규 인력 양성
- 재직자 실무역량 및 신기술 분야 보안 역량 강화
- 우수인재 발굴 및 육성을 위한 인력양성 기반 강화

Keynote 2



디지털 트랜스포메이션/Ontact 시대의 기업 정보보안

신수정 KT/Enterprise 부문장

코로나이슈와 4차 산업혁명으로 인해 디지털 트랜스포메이션이 급속히 진행되고 있다. 이에 따라 기업에서는 비즈니스의 변화, 일하는 방식의 변화, 디지털기술의 활용이 가속화되고 있다.

이러한 상황에서 기업 정보보안은 어떤 한계에 직면하고 있는지 또 어떤 방향으로 진화해야 하는지 고민이 있을 수밖에 없다. 본 강연에서는 그 방향으로 Agile, Flexible, resilient 의 세 가지 키워드를 제시한다.

교육세션

Tutorial 1
자동차 보안

자동차 내부네트워크 (CAN) 공격 및 탐지 방법론 교육

조효진 숭실대학교/교수, **최원석** 한성대학교/교수

2010년 IEEE S&P에서 발표된 자동차 해킹 가능성에 대한 연구 이후로, 다양한 자동차 해킹 사례들이 보고되었다. 이러한 해킹 사례들에 대응하기 위해서 국내외에서는 차량용 침입탐지 기술(Automotive Intrusion Detection System)이 연구·개발하고 있다.

특히, 2020년 UNECE의 자동차 사이버보안 국제기준 채택과 함께 Automotive IDS 기술에 대한 관심이 증가하고 있다.

본 교육에서는 자동차 내부 네트워크중 하나인 Controller Area Network (CAN)을 소개하고, 해당 네트워크를 통한 차량 제어등의 공격 방법론에 대해 살펴본다. 또한 대표적인 차량용 침입탐지 기술들을 소개한 후, 간단한 예제를 통해 IDS의 성능을 평가한다.

Tutorial 2
Security for AI

Deepfake 생성과 검출방법

정용현 삼성SDS/연구원

최근 딥러닝을 활용한 이미지 생성 기술의 발전과 더불어 이미지 생성 기술을 악용하는 딥페이크 사례가 이슈되고 있다. 딥페이크 이미지란 인공지능에 의해 합성된 이미지를 뜻하는 말로, 최근 다양한 범죄에 활용되기 때문에 딥페이크 이미지를 검출하는 연구가 광범위하게 진행되고 있다.

본 발표는 딥페이크가 어떻게 만들어지는지 알아보고, 올바른 활용 사례에 대해 논의 한다. 또한 딥페이크 이미지의 특징을 통해 딥페이크를 검출하는 최근 방법들에 대해 소개한다.

Tutorial 3
AI for Security

AI를 이용한 사용자 인증, 적대적 공격과 방어

최대선 숭실대학교/교수

본 강좌에서는 AI를 이용한 보안의 예로 사용자 인증을 소개하고, 이러한 AI 보안 시스템에 대한 적대적 공격과 방어 이슈를 설명한다.

AI 보안은 AI 자체의 안전성 이슈를 다루는 Safty of AI, 정보보호문제에 대한 AI 기반 솔루션을 제공하는 Security by AI, AI 자체의 취약점과 보안이슈를 다루는 Security for AI, 그리고 AI를 활용해 보안공격을 하는 Threats by AI 분야로 나눌 수 있다.

본 발표에서는 Security by AI의 일반적인 구성과 개발 흐름을 소개하고, 특히, 사용자 인증 분야에 AI 기술을 적용하는 구체적 방안과 사례를 설명한다. 또한, Security for AI 분야의 여러 가지 보안 위협과 이에 대한 대응 기술 들을 소개한다. 특히, 사용자 인증을 위해 사용된 AI 모델을 기만하는 공격에 대해 소개한다.

※ 해당 교육세션은 유료 교육으로, 유료교육 패키지 결제자에 한하여 수강 가능하십니다.

Session 1 / 300호

마이데이터/ 개인정보보호 이슈

혁신금융 마이데이터 산업의 비전과 개인정보보호

김태훈 뱅크샐러드/대표

정부와 관계 기관 및 산업의 적극적인 협력 속에서 데이터 산업의 기대와 중요성이 더욱 높아지고 있습니다. 데이터 경제 활성화로 나아가기 위한 토대가 마련되고 고객의 데이터 활용 및 통제 강화로 이러한 변화를 데이터 주인인 개인이 느낄 수 있을 만큼의 혁신적인 서비스로 이어가는 것이 이제 가장 중요한 때입니다.

뱅크샐러드는 핀테크 기업으로서 산발적으로 흩어져 있던 데이터를 일괄 관리할 수 있도록 하고 고객의 불편을 찾아 상식이 되어버린 불편함을 깨는 혁신을 만들어 가고자 합니다. 혁신적인 아이디어로 초개인화 된 서비스를 제공하고, 이런 아이디어와 서비스들을 지속적으로 결합시키면서 지금과 전혀 다른 새로운 서비스로 혁신을 만들어 갈 수 있도록 노력하고 있습니다.

뱅크샐러드가 바라보는 마이데이터 산업의 기회와 가능성, 그리고 정보전송요구권 도입 등으로 확대된 개인정보보호에 따른 책무와 역할에 대해 다룰 예정입니다.

공공부문 마이데이터 추진 동향과 이슈 분석

오강탁 한국지능정보사회진흥원/디지털정부본부장, 국민대학교/행정대학원 겸임교수

데이터를 기반으로 모든 분야의 디지털 전환이 가속화되고 있다. 특히 데이터 3법 제정으로 개인의 자기 데이터에 대한 주권을 기반으로 본인의 데이터를 관리 통제하고 이를 민원사무 처리, 건강관리 등 다양한 목적에 주도적으로 활용하는 마이데이터 사업이 민간뿐만 아니라 공공분야에서 주목을 받고 있다. 정부는 지난해부터 디지털 정부혁신 과제의 일환으로 행정과 공공기관에 흩어진 본인의 행정정보를 데이터 형태로 직접 받거나, 제3자에게 전송하도록 요구하여 활용할 수 있도록 공공부문 마이데이터 유통 체계 구축 사업을 추진 중에 있다. 최근 개인정보 전송요구 근거 마련을 위해 민원처리법을 개정하였고 개인정보보호법과 전자정부법 등 관련 법령의 개정도 진행 중이다. 그럼에도 불구하고 공공기관의 행정정보 전송요구권 대상 정보의 범위, 분야별 마이데이터 플랫폼간 연계, 국가 마이데이터 거버넌스 등 풀어야 할 다양한 정책 현안과 이슈가 있다. 따라서 본 발제에서 공공부문 마이데이터 추진현황과 전략에 대한 논의를 토대로 향후 확대 발전에 장애요인으로 작용할 수 있는 법제적·기술적 이슈의 내용과 해결 방향을 제안하고자 한다.

마이데이터와 개인정보자기결정권

권현준 한국인터넷진흥원/개인정보보호본부장

데이터는 4차 산업혁명 시대의 핵심동인 및 핵심자원으로 여기지고 있고, 특히 개인정보의 보호와 활용의 균형은 시대적 화두이다.

개인정보의 보호와 활용에 관한 이해관계자들의 역할이 기업 또는 기관 등 개인정보처리자 중심에서 개인, 즉 정보주체 중심으로 패러다임을 변화하고자 하고 움직임을 살펴보고, 이러한 흐름 속에서 정보주체의 자유와 권리의 근간으로 여겨지는 개인정보 자기결정권이 가지는 법제도적 의미를 살펴보고자 합니다.

Session 2 / 307호

CPS보안

제어시스템 이상징후 탐지 기술

서정택 가천대학교/교수

국가기반시설 제어시스템 운영 현황 및 정보보호 특성을 살펴보고, 제어시스템 대상 사이버공격 및 피해사례 분석을 통해 제어시스템 대상 공격의 특성을 확인한다. 이러한 보안위협에 대응하기 위한 제어시스템 이상징후 탐지 기술의 동향으로 국외 주요 연구과제 동향 및 NISTIR 8219 내용을 살펴보고, 국내에서 제어시스템 이상징후 탐지 기술로 연구개발되고 있는 동향 및 주요 기술을 소개한다.

마지막으로, 제어시스템 내에서 이상징후를 효과적으로 탐지하기 위한 도전과제를 제시한다.

기반시설 제어시스템에 대한 사이버 안전성 확보 전략

김신규 국가보안기술연구소/실장

에너지, 교통 등 국가 운영에 활용되는 기반시설 제어시스템에 대한 사이버 공격이 지속적으로 발생하고 있으며, 구성요소에 대한 공개 신규 취약점도 증가하고 있다. 따라서, 국가적으로 중요한 기반시설 제어시스템을 사이버 공격으로부터 안전하게 보호하기 위한 대책이 필요하다.

본 발표에서는 제어시스템의 특성과 국내 정책 현황을 고려하여, 기반시설 제어시스템의 구축단계부터 운영단계까지 사이버 안전성을 확보하기 위한 방안을 제시하고자 한다.

국내 스마트공장 보안강화 정책 동향

이향진 한국인터넷진흥원/팀장

5G 상용화 등으로 국내외 스마트공장 구축이 활성화됨에 따라, 이에 따른 보안위협도 증가하고 있음. 이에 따라 국내 스마트공장이 직면한 보안위협과 이에 대한 정부의 관련 정책을 소개하고, 정부 정책에 따라 추진 중인 국내 중소규모 스마트공장 대상 보안성 강화 지원 사업을 소개함.

Session 3 / 308호

차세대 이동통신 보안 (5G and beyond)

5G 엣지 네트워크 보안 기술

박종근 한국전자통신연구원/책임연구원

5G 엣지 네트워크는 단말과 물리적으로 가까운 기지국부터 지역 또는 광역국사까지의 초기 접속 구간을 말한다. 초고속·초연결·초저지연 5G 융합서비스의 활성화와 안전한 이용환경 보장을 위해 5G 엣지 네트워크에서의 보안 취약점을 식별하고 보안위협 대응 기술을 개발할 필요성이 크게 높아졌다.

본 발표에서는 5G 엣지 네트워크에서의 대표적인 보안위협과 이와 관련된 주요 기술 이슈 및 동향에 대해 살펴보기로 한다.

5G 이동통신 보안의 현재와 미래: NSA와 SA 보안 위협 중심으로

박성민 한국인터넷진흥원 / 책임

5G 이동통신은 지금 우리 실생활에 사용되고 있지만 아직 보안 관점에서 강화되어야 할 부분이 많이 있습니다. 특히 2G부터 시작된 이동통신에 대해 3G와 4G LTE를 거치면서 여러 가지 보안 위협들이 연구되었으며, 현재 조치 중이거나, 조치가 필요한 사항들이 많이 있습니다.

또한 5G 이동통신은 진화하고 있습니다. 현재 4G LTE 코어망을 유용하는 비독립망(NSA) 형태로 상용화 되어 있으며, 올해 독립망(SA) 형태의 진정한 5G가 상용화 될 것으로 예상되고 있습니다. 따라서 지금까지 연구되었던 5G 보안 위협들을 살펴보고 앞으로 상용화될 독립망에 대한 보안 위협들을 어떻게 대응해 나갈지 논의가 필요한 시점입니다.

5G기반의 스마트 팩토리 현황 및 보안 이슈

윤종필 에스케이텔레콤(주)/Project Manager

5G망 기술을 기반으로 제조 기업의 ICT기술 혁신에 일조하기 위해, '5G 인더스트리' 과제를 3년간 진행하였습니다. 5G 인더스트리 과제를 통해서 산업용 스펙의 5G 단말기를 개발하였고, 제조 현장에 적합한 공장 전용 사설(Private) 5G망을 국내 중견 제조 기업 7곳에 구축하였습니다. 본 강의에서는 제조 기업에서 활용 가능한 '5G망 기반의 생산 지원 서비스' 3종(자율 이송 로봇, 무선 기반 머신비젼, 설비 관리 증강현실)의 적용 현황을 설명하고, 진행과정에서 파악하게 된 기업들의 보안요구사항과 5G기술의 보안 관련 이슈를 설명드립니다

Session 4 / 401호

사이버보안 챌린지

Lessons learned from the Car Hacking and Defense Competition on In-Vehicle Network

조효진 숭실대학교/조교수

본 강연에서는 "K-사이버 시큐리티 챌린지 2020 - AI 보안 분야 자동차 해킹 공격/방어 트랙"의 참여 경험을 공유하고, 해당 챌린지에서 사용했던 차량 네트워크 공격 방법론 및 침입탐지시스템에 사용된 feature 선정 방법에 대해 소개한다. 또한 챌린지 대회에서 사용하지 못했던 공격 방법론을 추가적으로 소개하며, 해당 공격들에 대응하기 위한 후속 연구에 대한 진행 상황을 공유한다.

개인정보가 가명정보로 변하는 과정

박시온 윈스/주임

과학기술정보통신부가 주최하며 한국인터넷진흥원이 주관하는 국내 최대의 사이버 보안 분야 경연 대회인 'K-사이버 시큐리티 챌린지-2020'의 '개인정보 비식별 트랙'에 참가하고 수상한 경험을 바탕으로 해당 트랙과 경연을 준비했던 과정을 소개한다.

상세 내용으로는 개인정보 비식별 트랙에 대한 소개와 개인정보 비식별을 이해하는데 필요한 용어 설명, 그리고 경연에서 주어진 개인정보 데이터셋을 개인정보 분석 목적으로 활용하기 위해 가명정보/익명정보로 가공하는 과정과 도출한 결과에 대해서 설명한다.

Encrypted Traffic Analysis 기술동향 및 발전방향

김도연 호서대학교/연구원

네트워크 상의 보안성 강화를 위해 Encrypted HTTPS traffic의 사용량이 늘고 있다. 하지만 Encrypted Traffic에서 악성코드 배포, 데이터 유출 등 악성행위 또한 큰 폭으로 증가하고 있으며, 기존에 상용화되던 네트워크 보안기술은 HTTPS 환경에서 적용하기에 어려움이 있다. 이를 보완하기 위해 HTTPS Inspection 기술이 사용되고 있으나, 비용문제, CA 남용에 따른 위협 등 여러가지 이슈가 발견되었다. 이에 다양한 연구결과 분석을 통한 ETA(Encrpyted Traffic Analysis)의 기술동향 및 주요 응용 분야를 설명하며, TOR 환경에서의 실험 결과를 기반으로 ETA의 연구 가능성을 확인한다. 또한, 추후 ETA 연구 활성화를 위한 AI Dataset을 제안한다.

Session 5 / 300호

사이버보안 교육훈련

국제 사이버보안 교육 트렌드

김태성 충북대학교/교수

지능정보사회의 정보보호 위협이 가파르게 증가하고 있고 정보보호의 대상이 개인정보에서부터 민감한 군사정보에 이르기까지 매우 광범위해져, 숙련된 정보보안 전문인력의 역할은 더욱 커질 것임. 대응 전담팀을 별도로 운영하는 것이 매년 증가세에 있는 데이터 유출로 인한 피해를 감소시키는 가장 효과적인 방법으로 제기되고 있으며, 이로 인해 전문역량을 보유한 정보보안 전문인력의 확보가 중요해짐.

미국이나 영국 정부도 사이버보안 인력 부족문제(Shortage)를 심각하게 여기고, 교육·훈련의 강화를 통해 해결해 나가고자 노력하고 있음. 미국은 NICE Framework (https://niccs.cisa.gov/) 개발·보급을 통해, 영국은 CyBOK(Cyber Security Body of Knowledge; https://www.cybok.org/)의 개발·보급을 통해 국가에서 제공하는 초중고부터 대학(원)까지 및 재직자 재교육 과정의 모든 사이버보안 교육·훈련의 컨텐츠를 표준화하고자 노력하고 있으며, 실제 사이버보안 업무 현장에서의 경험을 가상체험하거나 인턴십 등을 통해 체화할수 있는 프로그램을 지속 발굴 중.

본 발표에서는 국가별 사이버보안교육의 현황과 트렌드를 분석하고 국내 사이버보안교육이 추구해야할 방향을 제시하고자 함.

국가공공기관 사이버보안 교육 현황

신욱 국가보안기술연구소/실장

국가보안기술연구소 사이버안전훈련센터는 국가공공기관, 주요정보통신기반시설 등 공공분야 인력을 대상으로 사이버보안 교육 및 훈련을 제공한다. 2012년부터 정보화 및 정보보호 업무를 담당하는 관리자와 실무자를 위해 사이버보안 관련 규정, 제도를 교육해왔으며, 특히 2014년 이후로는 공공분야 실무자들이 사이버공격·위협 대응 역량을 갖출 수 있도록 모사시스템을 바탕으로 공방훈련을 실시해왔다.

현재 사이버안전훈련센터는 교육 사각지대 해소를 위한 효과적·효율적인 교육 기반 확대 방안을 모색 중이다. 본 강연에서는 사이버안전훈련센터의 운영 이력과 앞으로의 계획을 공유한다.

사이버보안 훈련의 역할과 기술

김태일 ㈜코어시큐리티/대표이사

사이버 보안의 중요성이 날로 증가하고 있는 가운데, 최근들어 전 세계적으로 사이버 보안 훈련의 역할과 그 기능들이 새롭게 조명받고 있다. 과거 사이버 보안 훈련은 education, training의 개념에 치우쳐 지식 전달 및 스킬 숙달을 주 목적으로 하였으나 오늘날에는 exercise의 개념이 더 강조되어 지식 전달과 스킬 숙달이라는 전통적인 역할 이외에도 개인 및 조직의 사이버 보안 역량 진단과 개선을 위한 도구로서 활용되고 있다. 이러한 훈련 개념의 확장은 자연스럽게 그 목적을 달성하기 위한 기술들에 대한 연구 개발로 이어지고 있다. 본 강연에서는 오늘날 요구되는 사이버 보안 훈련의 역할을 살펴보고, 훈련 환경 구성부터 평가 및 진단에 이르는 다양한 기술들을 소개한다.

Session 6 / 307호

언택트 보안 & 블록체인

블록체인 기반의 디지털 ID 보관 및 연계 서비스 모델

박근덕 서울외대/교수

기존의 신원(ID) 인증 시스템(예: 분산 ID, 공동 인증서, 사설 인증서 등)은 다음과 같은 한계점이 존재한다.

- 보안이 취약한 모바일 기기(예: 스마트폰 등)에 악성코드 또는 해킹에 의한 ID 및 개인키 유출로 발생할 수 있는 신원 도용
- 이용자의 모바일 기기 분실 또는 도난에 의한 ID 및 개인키 유출로 발생할 수 있는 신원 도용
- 모바일 기기의 분실 또는 교체, 최악의 경우 ID 및 개인키 유출 시, 이미 발급 받은 ID의 수만큼 재발급 받아야 하는 불편함
- 분산 ID, 공개키 인증 기술을 가진 기업이나 사업자 별로 기술 구현이 서로 달라 신원 인증 시스템 간의 상호 연동이 어려움

이용자의 디지털 ID 및 개인키를 제3자에게 안전하게 저장 및 관리함으로서 신원 도용 방지 등 이용자 보호를 강화하고, 이기종의 신원 인증 시스템(예: 분산 ID, 사설 인증서, 공동 인증서 등)과 연동된 통합 ID(F-ID, Federation-ID)를 발급 및 공유하여 이용자 신원 증명 시 편리성을 극대화 할 수 있는 '블록체인 기반의 디지털 ID 보관 및 연계 서비스 모델'을 통하여 기존의 신원 인증 시스템의 한계점을 해결할 수 있다.

언택트 시대의 블록체인 활용 방안

이태영 한전KDN 전력ICT연구원/대리

전례 없는 코로나19 사태로 인해 우리사회는 최소한의 접촉만 허용되는 언택트 시대에 놓여있다. 비대면 시대에 맞춰 회의는 화상회의, 각종 평가는 비대면 평가 등으로 업무에도 많은 변화가 일어났다. 본 강연에서는 블록체인의 탄생 배경과 기본 개념을 먼저 설명하고, 코로나19로 인해 다시 뜨거워진 암호화폐 시장에 대해 알아본다. 마지막으로 언택트 시대의 블록체인이 어떻게 활용될 수 있는지에 대한 하나의 사례로 한전KDN에서 구축 중인 '블록체인 기반의 제안서 평가 시스템'에 대해 소개한다.

언택트 시대의 스위트홈 오피스 전략

김요셉 한국토지주택공사/CISO

원치 않더라도 출근을 잠시 멈추고 가정에서 끊이지 않는 업무전화만을 받고 있는 자신을 상상하게 되는 일상입니다.

착신전환 된 휴대폰만이 바로 사용가능한 업무 수단이라면?

스위트한 재택 오피스는 기업내부 보안과 동일한 보호대책이 가능하려면 어떻게 해야 할까요? 또는 내부 정책과 동일해야 할까요? 이러한 질문에 같이 고민하며 전략을 구체화 시켜 보겠습니다.

Session 7 / 308호

디지털포렌식

미국 소송에서 요구되는 전자문서 보존, 어디까지 해야하는가 (LG 에너지솔루션 vs. SK 이노베이션의 미국 소송을 중심으로)

심재훈 법무법인 혜명/외국 변호사

- 미국을 소송 무대로 선택할 경우에 신경써야 할 전자문서 보존의 특수성
- 전자문서 보존 의무가 시작되는 시점은 현실적으로 언제부터인가
- Litigation Hold를 받아본 적 있는가
- FRCP 26(f) Conference에서 약속할 전자문서 보존의 범위와 기간에 대한 사전 준비의 필요성
- 한국에서만 사용하는 특정 프로그램 (hwp, 카카오톡 등)과 한국 회사 내부에서 개별적으로 구축하고 있는 보완환경 등을 극복해야하는 전자문서 보존
- 전자문서 보존과 디지털 포렌식 서비스를 제공할 이-디스커버리 Vendor를 누가 선택해야 하는가
  (법무팀? IT팀? 보안팀? 소송 대리 국내 법무법인? 소송 대리 해외 로펌?)
- EDRM과 EDBP의 차이점은?
  (E-Discovery Reference Model vs. E-Discovery Best Practice)
- 소송대응 준비 상시화 프로그램 (Litigation Readiness)이 갖추어야할 전자문서 보존 정책과 가동 시스템
- 두 개의 미국 판례: Da Silva Moore vs. Publicis Groupe 에서의 TAR 판결과 Columbia Pictures vs. Bunnel 에서 metadata 판결
- 전자문서 보존 정책의 근간이 되어야 할 사내 (데이터 관리 정책)과 (인포메이션 거버넌스, Information Governance) 전략- 사전에 데이터의 생성부터 폐기까지 전 과정에서의 정보의 위치, 소유자, 보관기간 등을 명확하게 파악할 수 있도록 Data Map 만들기
- 전자문서 보존과 함께 미국에서 소송을 대리하는 미국 로펌에 설명해야 하는 우리나라 개인정보보호법의 특수성, 한국에서만 사용되는 파일형식, 시스템 특징 등에 대한 커뮤니케이션.

AI 기반 포렌식 선별(Triage) 기술

황현욱 국가보안기술연구소(NSR)/실장

최근 개정된 형사소송법의 검사와 사법경찰관의 상호협력에 관한 사항과 수사를 할 때 지켜야하는 일반적인 수사준칙의 규정에서도 살펴 볼 수 있듯이 국내 압수수색에서는 선별 압수를 기본 원칙으로 하고 있습니다. 이를 위해 수사관이 사용하는 현장용 포렌식 도구는 선별을 위한 기본 기능을 제공해야 합니다. 포렌식 전체 절차에서 선별(Triage)에 대해 정의하고 수사 관점에서 선별 기술을 설명하며, 그림 파일 선별시 AI 기반 기술을 적용하여 수사 목적에 맞게 선별의 정확도를 향상시킨 연구결과를 소개합니다.

자체 개발된 PRNG의 취약점을 이용한 랜섬웨어 복호화 기술 연구

박명서 국민대학교/연구원

랜섬웨어(Ransomware)는 데이터 보호에 사용되는 암호 알고리즘을 악용하는 악성코드(Malware)로써, 컴퓨터 시스템을 감염시켜 사용자의 문서, 사진, 동영상 파일을 암호화시키고, 복구를 위한 몸값(ransom)을 요구한다. 랜섬웨어는 불특정 다수를 감염시켰던 과거와는 달리, 최근에는 회사 또는 공공기관에 대한 타겟팅 공격이 증가하고 있다.

이러한 피해에 대처하는 방안 중 하나는 파일 감염에 사용되었던 암호화 키를 복구하는 것이다. 다수의 랜섬웨어는 PRNG (Pseudo Random Number Generator)를 암호화 키 생성에 이용한다. 암호학적으로 안전한 PRNG를 사용하면 암호화 키 복구가 불가능하지만, 간혹, 랜섬웨어 개발자가 자체적으로 개발한 PRNG를 사용하는 경우 암호학적 취약점을 이용하여 암호화 키 복구가 가능하다.

본 섹션에서는 자체 개발한 PRNG를 사용하는 랜섬웨어 중 하나인 Magniber v2의 취약점을 살펴보고, 이를 이용하여 감염된 파일에 대해 복구하는 방법에 대해 알아보고자 한다.

Session 8 / 401호

국내외 보안 챌린지 소개

사이버공격방어대회 소개

이상원 국가보안기술연구소/선임

사이버공격방어대회 목적, 연혁 등을 소개하고 대회 참여방법 및 진행절차 안내, 사이버공격방어대회 문제 소개, 2021년 개최 예정인 사이버공격방어대회 안내

산업제어시스템 보안위협 탐지 AI 경진대회(HAICon) 소개

민병길 국가보안기술연구소/실장

산업제어시스템 보안위협을 살펴보고, 이를 탐지하기 위한 AI기반 보안위협 탐지의 필요성과 장·단점을 설명합니다. AI기반 탐지 기술 개발에 있어 데이터의 중요성을 살펴보고, 이를 확보하고 분석하는데 있어 장애와 한계를 알아봅니다. 그리고 이를 해결하기 위해 국가보안기술연구소가 개발·공개한 HAI dataset에 대해서 설명하고, HAI dataset을 기반으로 개최한 "산업제어시스템 보안위협 탐지 AI 경진대회(HAICon)"의 소개와 2021년 개최 계획을 설명합니다.

국내외 제어시스템 보안 챌린지 대회 소개

문해은 ㈜NSHC/보안기술연구소장

최근 들어 OT영역에 대한 사이버보안에 대한 위협이 높아 지면서 제어시스템을 대상으로 하는 보안 챌린지에 대한 관심도 늘어나고 있다. 싱가포르에서 진행되는 CISS 대회, 미국 데프콘 컨퍼런스에서 진행되는 Red Alert ICS CTF, 국내에서 진행되는 산업통상자원 사이버보안 경진대회 등 각 대회의 특징을 살펴 보고, 왜 제어시스템의 보안 챌린지 대회가 필요한지, 앞으로 어떻게 발전되어야 하는지 고찰해 본다.

Session 9 / 300호

미래암호기술

ZKP 최신기술 동향

김지혜 국민대학교/부교수

* 4차 산업혁명으로 촉발되는 초연결 사회에서 신뢰성이 결합된 투명한 서비스에 대한 요구가 커지고 있음. 동시에 데이터의 프라이버시 보호가 중요해지고 있으며, 개인정보보호를 위한 법제화 및 권장사항들이 엄격해지는 추세임. 본 발표에서는 데이터에 대한 프라이버시를 유지하면서 데이터에 대한 임의의 정보를 공개적으로 검증할 수 있는 최신 영지식증명기술인 zk-SNARK(Zero-Knowledge Succinct Non-interactive Arguments of Knowledge)기술에 대해 살펴봄.

차세대 개인정보보호 강화 기술

조지훈 삼성SDS/마스터(상무)

전통적으로 데이터보안은 외부의 위협으로부터 데이터를 안전하게 보호하여 기업의 리스크를 최소화하는 방법론을 고민하였다. 하지만, 내부 부서간 혹은 외부와 데이터를 안전하게 공유할 수 있는 방안이 제공된다면, 데이터기반의 정확한 의사결정을 가능하게 하여 고객에게 양질의 서비스를 제공하거나 기업이나 조직의 생산성을 높일 수 있다.

개인정보나 혹은 조직 내 민감한 정보를 보호하면서 데이터를 공유하기 위해 비식별화 기술을 적용하고 있지만, 기존 비식별화 기술은 데이터를 훼손하여 데이터 가치를 현격히 떨어뜨리거나 타 데이터와 결합 시 재식별이 가능한 한계점이 존재한다. 이런 이유로 글로벌 기업들은 데이터 가치를 보존하고 높은 수준의 개인정보보호가 가능한 Privacy Enhancing Technologies(PETs)를 활발히 적용하고 있다. 본 발표에서는 이러한 PETs 기술과 Use Case를 소개하고자 한다.

PQC 전환 무엇부터 준비해야 하나?

강유성 한국전자통신연구원/실장

본 발표에서는 미래 암호시스템 인프라의 PQC(양자내성암호) 전환을 위한 단계적 접근방안을 소개한다. 당장 1~2년 사이에 등장할 가능성은 낮지만 고성능 양자컴퓨터에 의해 기존 암호시스템의 암호문이 해독될 수 있다는 위협이 존재하는 건 사실이다. 본 발표에서 설명하는 내용은 양자컴퓨터 시대를 대비하여 개발되고 있는 PQC 알고리즘을 실생활에 적용하는 암호시스템 인프라의 PQC 전환을 위한 준비내용과 관련이 있다. 본 발표는 현재 암호시스템의 양자컴퓨터에 의한 취약점을 분석하고, 미래 암호시스템 인프라 구축을 위해 PQC 알고리즘 개발과 함께 준비해야 하는 기술개발 방향성을 포함한다.

Session 10 / 307호

바이오 / 인증 보안

Biometric authentication / identification based on biosignals

이종실 한양대학교/연구교수

최근 모바일을 비롯한 다양한 스마트 기기들의 사용 증가와 더불어 다양한 개인정보들이 디지털화됨에 따라 정보보안에 관한 중요성이 강조되고 있다. 이에 따라 지문, 홍채, 얼굴 인식 기반의 생체 인식 기술은 많은 발전을 이루었다. 그러나 이러한 생체 인식 기술들은 사용자의 부재 시에도 사용될 수 있다는 단점을 가지고 있으며, 이를 보완하기 위하여 체온, 습도, 빛의 흡수나 반사, 동공 반응 등 추가적인 시스템을 요구하고 있다. 이에 반해 심전도와 광용적맥파와 같은 생체신호의 경우 개인 고유의 특성을 가지고 있으며, 살아있는 사람으로부터 기록되는 생체신호이기 때문에 위변조가 어렵다는 장점을 가지고 있다.

본 강연에서는 생체신호들 중 웨어러블 형태로 획득이 가능한 심전도 신호에 대하여 소개하며, 신호 획득 방법 및 이 신호를 이용한 인증 및 식별 연구에 대하여 소개를 하고자 한다.

분산 디지털 ID 관리 보안 기술

김수형 한국전자통신연구원/기술총괄

비대면 서비스의 일상화와 사회 전반에서 디지털 대전환이 가속화되고 있는 현재, 우리의 생활 속에서 다양한 형태로 빈번히 사용되고 있는 사용자의 신분증이 디지털화되고 온라인과 오프라인의 경계 없이 쉽고 편리하게 활용되는 디지털 신분증 시대가 도래하고 있다.

본 강연에서는 디지털 신분증을 구현하기 위한 핵심 기술인 분산 디지털 ID 관리 기술을 간략히 다루고, 디지털 신분증 활성화에 반드시 요구되는 보안 기술들을 소개하고자 한다.

디지털 뉴딜의 반도체 'swIDch Auth SDK'

최동근 센스톤/사장

〈도입〉
글로벌 혁신인증의 현주소, 지금 어디서 어떻게 활용하고 있는지와 활용할 수 있는지? 또한 카드번호 사기, AI스피커 도청, 드론 취약점 등 기존 인증의 문제점 등을 살펴보고, 패스워드 없이 접근할 수 있는 환경이 무엇인지 알아보는 기회가 될 것입니다.

〈본문〉
SDK 제공을 통한 인증보안 기술의 보편화를 통하여 1) 동일 솔루션을 공급하는 기업의 관련 R&D 인력을 보다 부가가치 높은 사업에 배치하고, 2) 고객의 내부시스템에 인증 솔루션을 구축하려는 기관과 기업은 이미 검증된 SDK 구매로 안정성과 효율성을 더욱 높일 수 있으며 3) SI기업들과 개발사 입장에서는 솔루션 구축 비용의 부담을 크게 줄일 수 있습니다.
swIDch Auth SDK 는 기술적으로 생체인증, 2단계 인증, 일회용 랜덤코드 인증 등을 모두 제공하고 있습니다. 3대 인증기능을 모두 갖춰 강력한 인증보안이 요구되는 상용솔루션부터 기업과 내부시스템 인증과 식별까지 효율적으로 적용할 수 있는 개발 Kit을 소개합니다.

Session 11 / 308호

양자 보안

최신 양자 컴퓨터 플랫폼 개발 현황과 현대 암호 동향

서화정 한성대/조교수

최근들어 글로벌 IT 대기업인 구글, IBM, Intel, 그리고 마이크로 소프트에서는 미래 컴퓨팅 기술인 양자 컴퓨터의 실용적인 구현을 위해 막대한 자본을 양자 컴퓨터 플랫폼 (양자 칩 및 양자 컴파일러) 개발에 투자하고 있다. 이는 양자 컴퓨터가 가지는 양자역학적 특징인 중첩과 얽힘 현상을 이용해서 현재 슈퍼 컴퓨터로는 해결하기 어려운 다양한 난제들을 해결하기 위함이다. 하지만 양자컴퓨터의 개발로 인해 수학적인 난제에 기반한 현대 암호 또한 해결됨에 따라 현존하는 암호화 시스템은 위기에 봉착할 것으로 예상된다.

본 강연에서는 현재 활용 가능한 다양한 양자 컴퓨터 플랫폼에 대해 소개하며 현대 암호에 대한 양자컴퓨터를 활용한 해킹 시도에 확인해 보도록 한다.

양자암호통신 연구동향 및 QKD 구축 기술

이원혁 한국과학기술정보연구원/선임연구원

– 최근 양자컴퓨터의 대두에 따른 기존 보안체계에 대한 위협에 대응하기 위한 산·학·연 중심의 여러 활동이 추진되고 있으며, 보안 알고리즘 적으로 대응하는 기법과 물리적 양자키 전달망으로서의 방안들이 적용되고 있다.

– KREONET은 국가 과학기술연구망으로서, 30여년간의 국가 공공 및 연구기관들이 밀집되어 서비스하고 있는 백본망으로서, 전용 네트워크 구축 및 보안관제를 중심으로 수행해왔으나, 최근 이슈에 맞추어 양자암호통신망 구축 기술을 연구하고 양자키를 안전하게 전달하기 위한 양자채널망 구축과 이를 활용한 양자암호통신망 구축 기술 연구를 수행중이다.

– 본 발표에서는 이러한 과정속에서의 국내 양자암호통신 연구동향에 대한 리뷰와 QKD구축기술을 활용한 국가 양자암호통신망 구축관련 진행에 대하여 소개한다.

〈Q|Crypton〉 암호 양자안전성검증 기술 개발 현황

이석준 한국전자통신연구원/박사/책임연구원

구글, IBM 등 세계 유수의 IT 기업들에 의해 양자컴퓨터가 본격적으로 개발됨에 따라, Shor 알고리즘, Grover 알고리즘 등 양자분석 알고리즘에 근거한 기존 암호체계의 위협이 커지고 있으며, NIST에서는 이에 대응하여 양자내성암호(PQC) 표준화에 속도를 내고 있다. 그러나 양자 알고리즘에 대한 양자컴퓨팅 처리 과정(양자 컴파일, 결함허용양자계산, 하드웨어 특성을 고려한 양자회로 배치 등)을 고려한다면, 이론적 양자 알고리즘과 실제 구현상의 간극이 존재하여 이를 반영한 암호 양자안전성검증 연구가 필요하다.

본 발표에서는 기존 암호 및 PQC 암호에 대한 양자안전성검증 연구 동향과 함께, ETRI에서 연구개발 중인 〈Q|Crypton〉 암호 양자안전성검증 기술 개발 현황을 소개한다.

Session 13 / 300호

자동차 보안 국제법규대응

자동차 사이버보안 국제 기준 및 향후 정책 방향

이은영 한국교통안전공단 자동차안전연구원/책임연구원

자동차에 전자제어장치가 증가하고 통신과 연결되면서 자동차 불법제어 및 프라이버시 침해 등 사이버보안 취약점과 위협이 매우 크게 증가하고 있다. 자동차에 대한 사이버공격 등 해킹의 피해는 최악의 경우 사망에 이르는 인명사고로 직접 이어질 수 있으므로 자동차 사이버보안 확보가 필수적이다. 따라서, 자동차 사이버보안 중요성에 대한 국제적인 공감대를 바탕으로 2020년 6월 UN WP.29(국제자동차기준 조화 회의체)에서 자동차 사이버보안에 관한 최초의 국제기준이 채택되었다.

본 강연에서는 자동차 사이버보안에 대한 국제 논의 현황과 우리나라 자동차 사이버보안 확보를 위한 향후 정책방향을 소개하고자 한다.

Comparative Study of Automotive Intrusion Detection Systems

최원석 한성대학교/조교수

2010년 자동차 해킹 가능성에 대하여 최초로 소개된 이후, 다양한 자동차 해킹 시나리오 등이 등장하였다. Charlie Miller와 Chris Valasek에 의하여 사전에 차량에 대한 수정조건 없이 원격에서 차량을 해킹할 수 있음을 시연하였다. 이러한 흐름 속에서 자동차 사이버 위협에 대응하고자 차량용 침입탐지 기술 (Automotive Intrusion Detection System)이 연구·개발되어 왔다. 특히, 2020년 UNECE의 자동차 사이버보안 국제기준 채택과 함께 Automotive IDS 기술에 대한 관심이 증가하고 있다. 본 발표에서는 자동차 해킹의 기본적인 원리에 대하여 알아보고 이를 탐지하기 위한 Automotive IDS 기술들에 대하여 설명한다. 특히, 지금까지 제안된 다양한 Automotive IDS들을 접근방법에 따라 분류하고 각 접근방법에 대한 장·단점을 살펴본다.

차량사이버보안 엔지니어링: 위험 평가 방법론

송윤근 이타스코리아 사이버보안사업팀/매니저

오늘날 자동차 산업계의 화두는 "차량 형식 승인"이다. 2022년 7월부터 모든 유럽 국가 및 1958 협정 체결국에 출시되는 신차는 "차량 형식 승인"을 받아야만 시장에 차량을 판매할 수 있게 된 것이다. 차량 제조사는 "차량 형식 승인"을 위해 사이버보안을 보장하기 위한 관리체계를 갖추고 증빙자료를 제출해야 하는데, 위험 평가 방법론도 그중 하나이다. 차량 제조사는 자신만의 위험 평가 방법론을 가지고 있어야 하며, 이를 기반으로 위험 평가를 수행하고 그 결과물을 제출해야 한다.

본 강연에서는 현재 제정중인 차량사이버보안 엔지니어링 표준인 ISO/SAE 21434에 기반한 위험 평가 절차 및 절차 별 요구 사항을 설명한다.

Session 14 / 307호

사이버위협 모델링&시뮬레이션

사이버 뉴노멀 시대의 위협헌팅전략

김혁준 ㈜나루씨큐리티/대표이사

K 방역의 성공은 한번도 방역의 중점을 질병대응에서 대한민국의 비즈니스 연속성 보장으로 확장했기 때문이다. 모두가 두려워하는 판대믹 상황에서 과학적 대응모델을 수립하여 질병의 탐지지점와 대응지점의 분리, 정량적 측정지표를 수립 및 과감하고 투명한 대응을 통해 전 국민을 설득하여 모두가 함께 대응할 수 있는 환경을 구성했고 획일적 기준을 제시하지 않고 급변하는 상황에 지표의 변화에 따라 능동적으로 대응하는 모습을 보여주었다.

본 발표에서는 K 방역의 성공요건을 사이버보안 환경에 적용하기 위한 증가하는 사이버위협 속에서 국가적 비즈니스 연속성 보장을 위한 사이버 위협헌팅 전략을 소개한다.

Adversarial Emulation, the next chapter.

노용환 주식회사 쏘마/대표

최근 고도화된 사이버 위협에 대응하기 위한 기술로 공격자의 행위를 에뮬레이션하는 기술이 많은 주목을 받고 있고, 이미 다양한 상용 BAS(Breach and Attack Simulation) 솔루션들과 유사한 성격의 오픈소스 프로젝트들이 있습니다. 공격자 행위 에뮬레이션(Adversarial Behavior Emulation)기술의 현재를 살펴보고, 해당 기술의 효율적인 사용방법과 앞으로의 연구 방향에 대해서 설명합니다.

시맨틱 공격 그래프 기술

이주영 한국전자통신연구원/책임연구원

최근의 사이버 공격에 있어서 공격자는 공격 대상 네트워크에 대한 정찰 및 탐색을 지속적으로 장기간 수행하여 정교한 공격을 시도하는 반면에, 방어자의 입장에서는 동적으로 빈번하게 변화하는 네트워크 환경으로 인해 자사 ICT 인프라의 보안 수준을 확신하지 못한다는 문제점이 있다. 이러한 문제를 극복하기 위해 주기적으로 ICT 인프라에 대한 Attack surface를 분석하는 것이 필요하며, 이를 통해 보안 취약점 뿐 아니라 부주의한 네트워크 설정 및 보안 정책에서의 오류 등을 검출하여 보안 강화를 위한 대응 방안을 수립할 수 있다. 이러한 Attack surface 분석에 사용할 수 있는 방법 중 하나인 공격 그래프 기술은 공격자가 타겟 네트워크 침입에 사용할 수 있는 경로를 표현하기 위한 모델을 정의하고, 이 모델을 기반으로 이용 가능한 모든 공격 경로를 식별하는 기술이다.

본 발표에서는 공격 그래프 기술과 공격 그래프 생성 방법 중 하나인 시맨틱 공격 그래프 기술에 대해 소개한다.

Session 15 / 308호

AI for Security

자연어처리를 통한 신규 위협정보 획득 및 처리기술 동향

류승진 NSR(국가보안기술연구소)/선임연구원

비정형 사이버 위협정보가 급격하게 증가함에 따라, 이에 대한 처리기술 수요 역시 증가하고 있다. 본 강연을 통해 비정형 자연어로 구성된 사이버위협 정보를 획득하고, 이를 분석하여 제공하는 AI 기술의 동향에 대해 살펴보도록 한다. 이를 위해 먼저 비정형 사이버 위협정보 대상 자연어처리의 필요성을 살펴보고, AI기반 최신 자연어처리 기술에 대해 간략히 설명한다. 마지막으로 보안분야 비정형 위협정보에 적용된 주요 자연어처리기술(임베딩, 데이터셋 구성, 개체명인식, 지식그래프 분석 등)을 기술 발전의 흐름에 따라 설명하고 본 강연을 마치도록 한다.

XAI 보안기술 분석 및 동향

서대희 상명대 지능데이터융합학부/교수

4차 산업혁명과 코로나19 팬데믹으로 언택트 환경에서 클라우드 및 빅데이터가 뒷받침 되면서 인공지능은 다양한 서비스로 개발되고 있다.

그러나 현재의 인공지능에서는 설계된 방식으로 출력값을 스스로 정하는 방식이었다. 따라서 심화신경망의 상호 작용 및 매개변수의 상호 작용은 사람의 인지가 불가능하며, 뛰어난 인공지능의 결과를 사람이 어떻게 받아들일지에 대한 문제와 더불어 결과의 신뢰성에 대한 문제성이 제기되었다.
이러한 문제를 해결하기 위하여 설명 가능한 인공지능에 대한 연구가 다양한 연구자들을 중심으로 활발히 진행되고 있다.

이에 본 발표에서는 기존의 인공지능의 문제점을 보완하기 위한 설명 가능한 인공지능을 소개하고 이를 이용한 보안 기술을 분석하고 연구 동향을 살펴보고자 한다.

AI 기술에 Plus, 보안을 Plus 하다

김의탁 ㈜이스트시큐리티/이사

다양한 사이버 위협과 이에 따른 수집 데이터의 급증으로 보안업체와 전문가들이 찾은 돌파구는 AI 기술을 보안에 접목하는 것이고, 이를 통해 많은 보안 인력과 분석가들의 업무를 대체하거나 축소하고 있다. AI 기술의 동향, Security 분야에 적용된 AI 기술 및 사례를 통해 변화하는 보안트렌드와 더불어 AI 기술에 대한 보안 위협과 데이터에 관한 보안 위협 동향을 분석한다.

Session 17 / 300호

위협 동향 및 코드분석 기법

안드로이드 앱 기반 피싱 탐지 동향

장민창 금융보안원/과장

금융보안원에서 운영 중인 피싱 분석 시스템 PAS(Phishing Analysis System)를 통해 지난해부터 최근까지 수집 분석된 안드로이드 앱 기반 피싱 동향을 다룬다.
PAS를 통해 수집되고 있는 악성 앱은 금융회사, 정부기관, 택배회사 등을 사칭하고 있지만, 대부분의 악성 앱은 금융회사와 정부기관을 사칭해 보이스피싱 범죄에 사용되는 전화가로채기용 앱이다. 이 유형의 앱은 2014년 처음 발견되었고 현재까지 변종이 계속해서 발견되고 있다.

이 강연에서는 수년간 지속되고 있는 보이스피싱 범죄의 핵심이 되는 악성 앱의 과거와 현재를 비교 분석한 내용과 보이스피싱 예방을 위해 능동적으로 대응하고 있는 내용들을 공유하고자 한다.

다크웹 내 범죄 에코시스템 동향

서현민 S2W LAB/수석연구원

다크웹은 일종의 범죄 에코시스템이 형성되어 해커들은 공급자와 수요자로 나뉘어 필요한 상품과 서비스를 개발하고 판매하는 형태로 이루어져 있다.

다크웹 내에 판매되는 악성코드, 계정 정보들은 실제 국내 침해사고에 활용된 사례가 있을 정도로 다크웹 내 컨텐츠들은 국내 사이버 침해사고에 직접적인 영향을 미치고 있으며, 관련 컨텐츠들은 현재도 활발히 생성되고 있다.

그 중 다크웹 내 해킹 콘텐츠들을 심층 분석하고, 침해 사례들을 참고해 선제적으로 대응할 수 있는 방안들에 대해 알아보도록 하겠다.

VMProtect Devirtualization via Symbolic Execution

박세준 Theori/CEO

프로그램 내에 포함된 지적재산을 보호하기 위해 리버스 엔지니어링과 디버깅을 어렵게 하는 코드 난독화를 적용합니다. 하지만, 이는 악성코드나 게임핵 등의 악성프로그램에도 적용되어 분석을 어렵게 하기도 합니다.

많은 상용 솔루션 중 오랜기간 동안 분석에 어려움을 주었던 VMProtect 3의 기능들을 살펴보고, Code Virtualization이 적용된 코드를 상대로 Symbolic Execution을 활용하여 자동으로 devirtualize 및 deobfuscate하여 다시 분석 가능한 형태로 난독화를 해제하는 방법에 대해서 설명합니다.

Session 18 / 307호

온라인게임 / 컨텐츠 보안

사설서버와 사이버 위협 인텔리전스

강병탁 (주)AI스페라/대표이사

원 게임을 그대로 시뮬레이팅하여 불법 서비스를 하는 프리서버, 사설서버 문제는 게임회사의 이미지에 타격을 주거나 영업상 큰 손실을 유발하는 등 게임업계에서 가장 대응하기 어려운 심각한 이슈 중 하나로 오래 전부터 인지되어 왔다. 요즘은 저작권 관련 정부 기관에서까지 관심을 갖고 불법 사설 서버를 탐지하고 차단하기 위하여 많은 노력을 기울이고 있지만, 해커들이나 사설서버 운영자들은 도메인과 IP를 지속적으로 변경하며 불법 운영을 하고 있는 탓에 어느 사이트에 어떤 사설서버를 서비스하고 있는지 파악조차 쉽지 않은 문제를 안고 있다.

본 강연은 사이버 위협 인텔리전스(CTI)를 이용하여 사설서버를 빅데이터와 인공지능 기반으로 탐지하고, 해당 사설서버를 폐쇄시키는 과정까지의 구조와 트랜잭션에 대해 설명한다. 전 세계 IP 주소와 불법 도메인 주소를 수집하여 사설서버를 판단하는 기술적 탐지 내용과, 여러 사설서버를 점조직처럼 운영하는 사설서버의 부모, 자식 사이트간의 관계, 그리고 머신러닝으로 불법서버를 탐지하는 기법 등 사설서버를 CTI 관점에서 분석하며 기술적 대응 히스토리를 소개할 예정이다.

인공지능을 이용한 게임커뮤니티 악성 글 탐지

우지영 순천향대학교/조교수

온라인게임 커뮤니티에서는 상대방에 대한 욕설, 모욕과 같은 toxic behavior가 발생하기도하고, 악성콘텐츠를 유포하는 통로로 활용되기도 합니다.

이러한 콘텐츠는 기업에서 발견즉시 삭제하므로 구축하기가 힘듭니다. 다만 커뮤니티에서 스캠인지를 질문하는 글이 발견됩니다. 본 발표에서는 국내외 게임 커뮤니티에서 스캠관련 글을 수집하며 스캠글의 특성을 파악하여 인공지능 기반으로 자동으로 스캠을 탐지하는 모델을 개발을 내용을 소개합니다.

Weak supervised learning을 이용한 작업장 탐지 (신뢰도가 부족한 Label 개선 방안)

조양규 엔씨소프트/팀원

엔씨소프트 모바일 게임 내의 작업장 탐지 모델링 과정에서 부정확한 Label 개선 방안을 위해 Weak supervised learning 기법을 적용한 분석에 대한 발표입니다.

기존 작업장 탐지 모델링 과정에서는 여러 사유로 인해 정확한Label 정보를 얻기 어려운 점이 있었으며, 이러한 부정확한 Label을 통해 학습된 모델의 한계가 있었습니다.

따라서 Snorkel이라는 Weak supervised learning 관련 기법이 구현된 라이브러리를 통해, 부정확한 라벨을 보완한 뒤 효과 검정 까지 한 사례에 대한 내용을 다루고자 합니다.

Session 19 / 308호

Security for AI

딥러닝 적대적 예제와 퍼징 기술

권태경 연세대학교/교수

딥러닝의 발전과 성공은 자율주행과 같이 안전이 중요한 시나리오에 심층신경망을 효과적으로 적용하는 시대를 앞당기고 있다. 적대적 예제라 부르는 기교적 입력에 대한 심층신경망의 숨겨진 취약점은 따라서 시대적 위협이 될 수 있다. 소프트웨어엔지니어링 문제에 딥러닝을 적용하는 분야뿐만 아니라 그 반대의 경우도 다양한 기술 접목이 이루어지고 있다. 소프트웨어의 숨겨진 취약점을 효과적으로 찾는 기술인 커버리지 기반 퍼징의 유용한 개념을 이러한 심층신경망의 잠재적 결함을 찾는데 활용하는 기술을 살펴보고 그 가능성과 한계를 알아보도록 한다.

Confidential computing for data protection

이병영 서울대학교 전기정보공학부/부교수

본 발표에서는 데이터를 보호하기 위한 기밀계산(confidential computing)을 활용한 새로운 어플리케이션 디자인 방법을 소개한다.

개인 정보를 보호하는 네트웍 서비스, 개인 정보를 보호하는 데이터베이스, 개인 정보를 보호하는 AI/DL 서비스 등 기존의 컴퓨팅 서비스를 더욱 안전하게 하기 위한 솔루션들을 소개한다. 또한 Google Cloud, MS Azure, Amazon EC2 등의 클라우드 서비스에서의 기밀계산기술 적용 현황과 이와 관련한 하드웨어 기술들인 Intel SGX, Intel TDX, AMD SEV 등의 기술에 대한 소개와 앞으로의 미래에 대한 전망을 소개하고자 한다.

공격에 강인한 심층인공신경망 구조 연구

김현우 고려대학교 정보대학 컴퓨터학과/조교수

심층인공신경망을 공격에 강인하게 만들기 위하여 널리 사용되고 있는 인공신경망의 구조를 개서하는 방법을 제안한다.

널리 사용되고 있는 ResNet 구조는 오일러 이산화 연산을 인공신경망으로 변환한 것으로 해석될 수 있는데 강안정성을 제공하는 보다 안정적인 이산화 방법을 인공신경망의 구조에 접목하여 안정성을 향상 시킨다. Strong Stability Preserving (SSP)을 활용하여 새로운 인공신경망 구조를 제안하고 적대적 공격에 강인함을 실험과 이론을 통해 연구한다.

특별세션

인재양성 1

차세대 암호기술: 함수암호 개요 및 응용

서민혜 덕성여자대학교 사이버보안전공/조교수

함수암호는 프라이버시를 보호하면서 암호화된 데이터에 대한 연산을 수행할 수 있는 진화된 형태의 암호기술로, 암호화된 데이터에 대해서 연산을 수행하고 그 연산의 결과를 평문 형태로 얻을 수 있는 새로운 공개키 암호 기법이다.

비밀키를 가진 수신자에게 평문을 전부 제공하는 기존의 암호와 달리, 함수암호는 특정 연산에 대응되는 비밀키를 가진 수신자에게 평문에 대한 연산 결과만 제공한다. 본 발표에서는 함수암호에 대한 기본적인 개념을 설명하고, 함수암호를 적용할 수 있는 다양한 응용환경을 소개한다.

Using sonar for liveness detection to protect smart speakers against remote attackers

이연준 한양대학교/조교수

Smart speakers, which wait for voice commands and complete tasks for users, are becoming part of common households. While voice commands came with basic functionalities in the earlier days, as the market grew, various commands with critical functionalities were developed; e.g., access banking services, send money, open front door. Such voice commands can cause serious consequences once smart speakers are attacked. Recent research shows that smart speakers are vulnerable to malicious voice commands sent from other speakers (e.g., TV, baby monitor, radio) in the same area. In this work, we propose the Speaker-Sonar, a sonar-based liveness detection system for smart speakers. Our approach aims to protect the smart speakers from remote attackers that leverage network-connected speakers to send malicious commands. The key idea of our approach is to make sure that the voice command is indeed coming from the user. For this purpose, the Speaker-Sonar emits an inaudible sound and tracks the user's direction to compare it with the direction of the received voice command. The Speaker-Sonar does not require additional action from the user and works through an automatic consistency check. We built the Speaker-Sonar on a raspberry pi 3b, a circular microphone array, and a commodity speaker by imitating the Amazon Echo. Our evaluation shows that the Speaker-Sonar can reject remote voice attacks with an average accuracy of 95.5% in 2 meters, which significantly raises the bar for remote attackers. To the best of our knowledge, our defense is able to defend against known remote voice attack techniques.

디버깅 기능을 활용한 모바일 보안 기술

장진수 충남대학교 컴퓨터융합학부/조교수

Samsung RKP와 같은 커널 무결성 보호 기술은 하드웨어 지원 가상화 또는 TrustZone과 같은 CPU 보안 기술을 바탕으로 구성된 신뢰 실행 환경을 신뢰 기반으로 구현되어 있다.

이러한 신뢰 실행 환경은 일반 실행 환경과의 격리를 통해 신뢰 실행 환경 내에 적재된 보안 솔루션들을 공격자로부터 보호한다. 하지만 격리된 보안 소프트웨어도 취약점을 수반할 수 있으며, 이를 악용한 공격 성공 시, 보안 소프트웨어의 무결성이 손상될 수 있다. 이러한 문제를 해결하기 위해 범용 하드웨어인 와치포인트와 쓰기 영역 실행 방지(DEP)기능을 활용한 신뢰 실행 환경의 내부 특권 분리 기술을 소개한다.

해외 주요국의 알고리즘 규제 논의와 법제도 동향

김법연 고려대학교 정보보호대학원/연구교수

인공지능의 위험성은 이미 지속적으로 경고되어 온 것으로 이 문제를 해결하기 위해 해외 각국은 윤리적, 규범적 논의를 다양하게 실시하고 있다. AI 기술에 대한 위험에 대응하기 위해 윤리적 규범과 원칙이 제시되고 있고 법률적·규제적 통제가 본격화되고 있기도 하고 있다. 이러한 AI와 알고리즘에 대한 규제는 데이터 이용에 있어서의 적정성과 공정성, 데이터 분석결과에 대한 책임성과 투명성 등이 강조되고 있지만 이용자의 프라이버시나 개인정보보호, 사이버보안에 대한 리스크 감소를 위한 규제조치들도 구체화되고 있다.

이에 본 발표에서는 해외 주요국의 AI 및 알고리즘 규제동향과 정보보호 분야에 있어서의 정책적 쟁점과 이슈 등에 대해서 살펴보고자 한다.

인재양성 2

The Abuser Inside Apps: Finding the Culprit Committing Mobile Ad Fraud

손수엘 한국과학기술원/손수엘

Mobile ad fraud is a significant threat that victimizes app publishers and their users, thereby undermining the ecosystem of app markets. Prior works on detecting mobile ad fraud have focused on constructing predefined test scenarios that preclude user involvement in identifying ad fraud. However, due to their dependence on contextual testing environments, these works have neglected to track which app modules and which user interactions are responsible for observed ad fraud.

To address these shortcomings, we present the design and implementation of FraudDetective, a dynamic testing framework that identifies ad fraud activities. FraudDetective computes a full stack trace from an observed ad fraud activity to a user event by connecting fragmented multiple stack traces, thus generating the causal relationships between user inputs and the observed fraudulent activity. We evaluate FraudDetective on 48,172 apps from Google Play Store. FraudDetective reports that 74 apps are responsible for 34,453 ad fraud activities and find that 98.6% of the fraudulent behaviors originate from embedded third-party ad libraries. Our evaluation demonstrates that FraudDetective is capable of accurately identifying ad fraud via reasoning based on observed suspicious behaviors without user interactions. The experimental results also yield the new insight that abusive ad service providers harness their ad libraries to actively engage in committing ad fraud.

해외 주요국 개인정보 비식별화 법제도 동향

주문호 고려대학교 정보보호대학원/연구교수

개인정보의 활용의 가치와 안전한 활용 요구가 동시에 높아지면서 해외 주요국들은 데이터의 활용성을 높이기 위한 개인정보 비식별화에 초점을 맞춘 새로운 법률과 정책을 도입하고 있습니다.

이에 본 발표에서는 최근 유럽 연합, 미국, 일본, 한국이 개인정보보호법에 어떻게 비식별화 개념을 도입하고 있는지 비교·분석하고 공통된 경향과 시사점을 제시하고자 합니다. 특히 비식별화의 법적 개념과 비식별정보의 취급, 데이터 컨트롤러 의무 및 비식별 절차를 비교하여 향후 비식별 정책의 발전 방향을 예측합니다.

딥러닝 모델에서의 적대적 사례 연구

권현 육군사관학교/조교수

딥뉴럴네트워크 기반의 딥러닝 모델은 보안상 취약점이 존재한다. 취약점 중에 exploratory attack은 이미 학습이 끝난 모델에 대하여 테스트 데이터를 조작하여 모델의 오인식을 유발하는 공격방법이다. exploratory attack은 테스트 데이터를 조작하는 방법으로 모델에 의해 잘못 오인식이 되는 샘플이기 때문에 현실성이 높은 공격방법이 된다.

이러한 exploratory attack의 대표적인 예로 적대적 사례가 있으며 이번 강연에서는 적대적 사례에 관련한 연구에 대해서 소개할 예정이다.

법률지원

개인정보 분쟁조정 현황 및 개선방안

윤여진 개인정보위원회/분쟁조정과장

개인정보 관련 분쟁을 소송외적으로 원만히 조정하기 위해 2001년에 처음으로 개인정보 분쟁조정제도를 도입하였고, 2016년 7월 한국인터넷진흥원에서 개인정보 분쟁조정위원회를 운영하던 것을 개인정보보호위원회로 이관하였다. 중요 분쟁조정사례를 소개하고, 최근 4년간 개인정보 분쟁조정제도의 성과 및 한계를 분석하며 개인정보 분쟁조정제도가 나아갈 방향을 제시하고자 한다.

개인정보는 분쟁조정은 정보주체가 쉽고 신속하게 개인정보의 침해를 구제받을 수 있는 제도인 바, 앞으로 개인정보의 중요성과 비례하여 분쟁조정위원회의 역할도 확대될 것으로 기대한다.

공공데이터제공 분쟁조정제도와 사례

정종열 한국지능정보사회진흥원/연구위원

공공데이터 제공 및 이용활성화에 관한 법률에 따라, 국가 및 공공기관이 보유하고 있는 데이터 중, 개인정보, 영업비밀 등 비공개정보와 제3자 권리가 포함된 정보를 제외한 모든 데이터를 국민에게 제공토록 하고 있다. 이 과정에서 공공기관이 공공데이터 제공을 거부하거나 중단하는 경우, 국민이 간단한 분쟁조정 절차만으로 데이터 이용권리를 구제받을 수 있도록 만든 분쟁조정제도와 주요 분쟁조정 유형별 사례를 소개함으로써 공공데이터 제공과 관련된 분쟁해결뿐만 아니라 분쟁의 예방 및 사전 문제해결에 도움이 될 수 있도록 한다.

저작권보호심의제도와 사례

오진해 한국저작권보호원/저작권보호심의위원회 전문위원

한국저작권보호원 저작권보호심의위원회는 저작권법 제133조의2 및 제133조의3에 따른 불법복제물등의 삭제·전송중단과 복제·전송자에 대한 경고 등의 시정명령·시정권고의 심의, 동법 제103조의3에 따른 복제·전송자에 대한 정보제공명령청구의 심의를 담당합니다.

시정권고의 심의를 통해서는 온라인에서 매우 빠르게 확산되는 불법복제물에 의한 저작권 침해를 온라인서비스제공자의 자율적 조치로 신속하게 차단하고, 저작권법을 잘 알지 못하는 이용자들에게 저작권법 위반을 미리 알려 저작권 분쟁을 사전에 방지하고자 합니다.

정보제공명령청구의 심의를 통하여는 저작권자 입장에서는 권리 실현을 위하여 복제·전송자의 정보를 획득하는 데 겪는 어려움을 해소하고, 또한 이용자 입장에서는 개인정보보호와의 균형을 꾀하고자 합니다.