제52회 KISTEP 수요포럼 주요 내용

2016. 9

KISTEP 한국과학기술기획평가원
Korea Institute of S&T Evaluation and Planning

1. 개요

□ **일 시** : 2016년 9월 21일(수) 10:00~12:00

□ **장 소** : 한국과학기술기획평가원 12층 국제회의실

□ **발표자** : 이경호 고려대학교 교수

□ **주 제** : 지능정보사회로의 진전과 사이버 보안 미래 과제

□ **토론자** : 정수환 숭실대학교 교수
이재일 정보통신기술진흥센터 정보보호 CP
황보성 한국인터넷진흥원 단장

시 간	내 용	비 고
10:00~10:05	개회사	박영아 한국과학기술기획평가원 원장
10:05~10:10	발표자 소개	(사회) 황지호 한국과학기술기획평가원 본부장
10:10~10:50 (40분)	주제 발표	곽재원 경기과학기술진흥원 원장
10:50~11:30 (40분)	패널소개 및 지정 토론	(좌장) 황지호 한국과학기술기획평가원 본부장 (패널) 정수환 숭실대학교 교수 이재일 정보통신기술진흥센터 정보보호 CP 황보성 한국인터넷진흥원 단장
11:30~12:00 (30분)	자유 토론	참석자 전원
12:00	폐회	(사회) 황지호 한국과학기술기획평가원 본부장

2. 주제 발표 주요 내용

□ 발표 주제: 지능정보사회로의 진전과 사이버 보안 미래 과제

□ 대한민국의 통신, 금융환경

○ 2016년 대한민국의 통신환경

- 이동전화 가입자수 약 6000만 명으로 경제활동 인구의 2배, 특히 스마트폰 가입자가 4300만 명
- 이동통신 가입자 중 91%가 무선인터넷 이용 중, 이동통신 환경이 스마트폰으로 넘어갔고, 언제 어디서나 움직이며 무선 인터넷 접근이 가능해짐

○ 2016년 대한민국의 금융환경

- 인터넷뱅킹 일일거래액 40조 중 모바일 뱅킹 이용 비중이 54% 넘어섬
- 금융서비스 업무처리 비중 중 창구거래 약 10%, 인터넷뱅킹 80%
- 모바일 뱅킹 이용 비율 36%, 특히 최근 6개월 이내 처음 시작 비율이 30%로 변화가 급속도로 이루어지고 있음

○ 모바일, 인터넷 금융 확대와 보안 문제

- 모바일뱅킹 이용 이유는 편리함이 51%, 이용하지 않는 가장 큰 이유는 개인정보 유출 우려, 안전장치 불신 등 보안문제
- 인터넷결제 시 실제 보안 관련 사고로 인한 금전적 손실 경험은 0.4%로 굉장히 적고, 신용카드 부정사용 비율도 선진국과 비교할 때 10배 이상 우리나라 부정사용 비율이 낮음
- 한국은 사고 경험은 거의 없지만 정서적 불안 문제가 큰 상황

□ 클라우드와 공공데이터 개방

○ "클라우드컴퓨팅"(Cloud Computing)이란 집적·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원(이하 "정보통신자원"이라 한다)을 이용자의 요구나 수요 변화에 따라 정보통신망을 통하여 신축적으로 이

용할 수 있도록 하는 정보처리체계를 말함

○ 한국의 클라우드 컴퓨팅

- 클라우드 컴퓨팅 발전법의 통과 및 시행. 2015년 3월 공포
- 공공기관 도입 확대, 산업 발전기반 조성, 클라우드로 비용 절감, 신속한 조치 가능 등 긍정적 기능
- 이용자 개인정보 보호 등 역기능을 방지하기 위한 고민 필요

□ 매직 키워드-핀테크

○ 금융을 뜻하는 파이낸셜(financial)과 기술(technique)의 합성어로 모바일 결제 및 송금, 개인자산관리, 크라우드 펀딩 등 정보기술(IT)을 기반으로 한 새로운 형태의 금융 기술

○ 금융의 본질을 구가함에 있어서 기술을 어떻게 활용할지 고민하여 핀테크가 이런 리스크를 줄여준다면 안정과 수익 창출 가능

○ 전자금융 주요 참가자들 중 굉장히 다양한 플레이어들이 각축전을 벌이고 있는데 이 안에서 어떤 모델을 찾아낼지가 문제

□ 해킹 및 정보 유출 사고들

○ 방글라데시 은행 해킹 사건

- 올 해 2월 초 방글라데시 은행에서 약 1,000억 원이 해킹됨
- SWIFT 메시지 해킹: 해당 악성코드는 발송자가 8개 은행의 특정조건에 해당할 경우, 인터페이스 화면상의 금액을 조작하여, 부정 거래 사실을 은폐하는 기능이 포함
- 유사한 시도가 작년에도 있었고, 우리나라 은행들도 같이 연루됨

○ 한국의 인터파크 해킹 사건

- 그렇게 높은 수준이 아니라 일상적인 수준에 당함
- 이런 역기능을 제대로 커버하지 못하면 새로운 기술을 제대로 이용하고 접목할 수 있을지 의문

○ 한국의 악성코드 감염

- 2013년 전 세계에서 악성코드 감염이 가장 많은 지역 1위가 한국으로 사고가 안 나는 게 이상한 지경이었고, 증가 비율도 한국이 최고였음
- 사고 이후 2014년 악성코드 감염으로 초점이 맞춰지고 한국의 상황이 많이 개선되고 안정화 되어가고 있음

○ 그러나 여전히 새로운 공격방법들의 경연장이며 최근에는 랜섬웨어 등 첨단 범죄들의 타겟

- 랜섬웨어: 시스템에 저장된 문서들을 암호화 시킨 후 복호화를 위해 금전을 요구하는 목적으로 제작된 악성코드로 암호화를 위해 외부의 C&C 서버와 통신하며, 주로 문서파일들을 암호화
- 한국은 세계 3위, 2016년 3월 1일 ~ 27일까지 국내 100,000건 이상의 Locky 랜섬웨어 유입 탐지

□ 국가의 데이터 활용

○ 치머만 전보, 제로니모 작전 등 암호가 역사를 바꾼 사례들

○ 에셜론: UKUSA 5개 회원국(AUSCANZUKUS: 오스트레일리아, 캐나다, 뉴질랜드, 영국 그리고 미국)이 운영하는 전 세계의 통신을 감청하는 신호정보 수집 및 분석 네트워크

○ 정보 분석력이 곧 국가 경쟁력

- 미국은 빅데이터와 최고의 기술력을 보유한 기업들과 협업하여 사이버 패권을 꿈꾸고 있고 이미 악성코드를 활용한 블랙마켓이 운영되고 있으며 실제로 작전에 활용하고 있음

□ 정보와 개인정보

○ 개인정보

- 정보란 국가의 의지를 표현하는 데 가장 중요한 수단 중 하나로 특히 개인정보가 중요

- 개인정보의 정의는 생존하는 개인에 관한 정보로서 당해 정보에 포함되어있는 성명, 주민번호 등으로 개인을 식별할 수 있는 정보
- 근래들어 기존 개인정보 개념이 인격권과 재산권이 혼재된 새로운 개념으로 범위가 급속도로 확대되고 있음

○ 개인정보의 보호와 빅데이터

- 개인정보 유출은 개인의 정신적•경제적 피해를 야기할 뿐만 아니라 정보사회 자체에 대한 신뢰를 붕괴하여 사회적 혼란이 야기될 수 있음
- 그러나 디지털 강국으로 가는 과정에서 개인정보의 비식별화를 통해 빅데이터에 이용할 수 있도록 개인정보 보호법의 섬세한 개정 필요

□ 결론: 레거시의 붕괴와 새로운 전략

○ 공격은 알려지지 않은 방식으로 시작되기 때문에 방어체계 틀 자체도 유연하게 변해야 하며, 다양한 도구를 활용할 필요성

- 알려진 공격(Known attack)은 ID/PW 도용, 툴에 의한 해킹 등과 같이 잘 알려지고 빈번히 일어나는 정보 침해 공격을 말함
- 알려지고 기록되지 않은 취약점을 타겟으로 일어나는 알려지지 않은 공격(Unknown attack)을 막기 위해서는 비정상행위탐지(behavior-based anomaly detection)를 사용 함
- 기존에 대비하고 있는 알려진 중요정보 침해에 비해 Impact가 큰 알려지지 않은 중요정보 침해에 대한 관리가 필요함
- 현재의 인력 및 기술로는 신종(변종) 공격패턴 출현 시 즉각적인 대응이 곤란함
- 머신러닝 기술을 활용하여 시스템이 스스로 학습해 이상행위를 탐지해내는 알고리즘을 개발할 필요성

○ 딥러닝과 인공지능을 기반으로한 데이터 과학이 결합하여 첨단 범죄에 대응하고 국가 안보에 활용되는 시대가 이미 도래했고 더욱 발전할 것인데 우리 모두가 이러한 시대에 국익을 보호하고 글로벌 경쟁에서 산업을 보호하기 위하여 국가의 기반 인프라로서 사이버 보안 산업에 투자와 관심을 기울여야 함

3. 패널토론 주요 내용

【 정수환 교수, 숭실대학교 】

□ 새로운 시대에 급부상중인 두 지능: 집단지성과 인공지능

○ 현대 사회를 빠르게 바꾸고 있는 집단지성과 인공지능이 해커 세계에서도 활용되고 있으므로 대응 체계도 이에 따른 전환 필요

- 해킹 자체를 서비스로 제공하는 클라우드 집단도 있고, 취약점을 찾는 detection tool 이용해 해커들이 협업하는 시대로 가고 있음
- 해커들이 집단 지성과 인공 지능을 활용하고 있는 시대에 과거의 패러다임으로는 대처불가, 새로운 패러다임 필요
- 오픈 플랫폼 기본의 집단 지성과, 사람들이 미처 다 분석하지 못하는 것을 분석하도록 하는 인공지능 두 가지 모두를 활용하는 플랫폼을 만들어야 함

○ 전 세계 보안 회사들은 이러한 작업을 하기 위한 인프라들이 많이 갖춰져 있는 반면 우리나라는 취약한 실정에서 새로운 국가적 사이버 보안 플랫폼이 필요함

- 기관별로 데이터를 수집하고 있지만 공유 체계가 부족, 수집 양 자체도 적고, 위험 데이터를 식별할 수 있어야 하며 민간 기업들도 참여하도록 해야 함
- 하루에도 수 테라바이트씩 생산되는 정보를 인간이 다 분석할 수 없으므로 인공지능의 발전이 필요함

【 이재일 정보보호 CP, 정보통신기술진흥센터 】

□ 지능정보 사회에서의 보안문제

○ 지능정보 사회에서 이것이 우리에게 미칠 사이버 보안 문제와, 이를 이용한 보안 활용이라는 두 가지 관점에서 바라봄

- 4차 산업혁명은 인공지능이나 로봇이 도입되며 산업의 새로운 혁명을

촉발했고, 사이버와 물리 시스템이 만나 굉장히 편리해지면서 동시에 일상과 사이버가 타이트하게 접목되게 됨

- 지능정보사회에서 편리성만이 아니라 개인에게도 큰 위협이 될 수 있음
- MS에서 만든 채팅로봇의 학습이 오염되어 나치주의자들과 인종차별적인 오작동을 해 사용 중단된 사건은 외부 입력에 의해 AI가 고의적으로 오작동 된 사례
- 인공지능은 학습 단계를 거쳐야 하는데 소프트웨어 오류뿐만 아니라 악의적인 데이터 도입 시 평상시엔 정상 운영하다 고의적인 잘못된 학습에 의해 결정적 순간에 치명적 영향을 미칠 수 있음
- 인공지능에서 다량의 학습 데이터가 이용되며 큰 프라이버시 문제가 될 수 있기에 그런 문제를 피하며 다량의 학습을 할 수 있는 방법을 고민하고 준비해야 함

【 황보성 단장, 한국인터넷진흥원 】

□ 해킹 환경의 다변화에 따른 대응 방안 필요

○ 해킹 공격 현황

- 핵실험 이후에 정부 인사나 주요 기관 시설에 대한 해킹 시도들이 상당했고, sns나 블로그 등 비정형데이터를 통해 다양한 해킹 시도가 이루어지고 있음
- 해킹이 천재적인 능력이나 기술이 없어도 시스템을 다운받아 누구나 공격할 수 있는 환경이 되어 탐지, 분석, 대응해야 하는 기계가 너무 많아져 분석가, 대응가들이 하나씩 처리할 수 있는 환경이 아님

○ 인공지능과 사이버 보안 결합 필요

- 초기에 사이버 보안 문제는 독자 방어였으나, 2세대 방어 체계는 보안업체나 유관기관의 정보 공유 intelligence 협업 방안이며 앞으로 거대한 데이터를 처리하기 위해서는 협업 + 인공지능이 결합되어야 함
- 구글의 알파고처럼 IBM은 왓슨에 해킹 정보를 공부시키고 있음. 궁극

적 목표는 최대한 인공지능 기능을 발달시켜 내부와 외부의 위협정보를 결합해 사이버 위협 정보를 탐지해 대응하여 현재 사람이 1에서 10까지 다 처리하는 방식에서 인공지능이 1-5정도까지는 하는 것을 목표로 하고 있음

- 인공지능과 사이버 보안을 결합시키는 절차 3가지. 1) 각자의 정보를 하나의 플랫폼에 담는 클러스트화 2) 분석가들의 경험을 최대한 학습시키는 딥러닝 통해 해킹 사고 개요를 자동 분석화 3) 자동 분석된 데이터를 이용해 최종 예측

【 기타 의견 】

□ 북한의 사이버 공격 위협을 전문가들이 어느 정도의 수준으로 평가하고 있는지?

⇒ 북한의 사이버 공격 역량은 지금까지의 자료로는 최근 6800명 가량의 사이버 전사를 양성 중이며 교육체계는 영재중, 영재고, 전문화된 대학들에서 양성하고 있음. 후에 군 조직이나 중국 등지의 회사에 들어가 평시에는 한국의 사이버 공간 개인정보 수집 등 다양한 활동을 하며 외화벌이 사업을 하다 결정적 순간에 활용하고 있음

⇒ 북한의 사이버 역량을 미국 당국자가 상당히 높게 평가하고 있음. 기술역량은 미국 등을 따라오지 못하지만 공격하는 기획력이 좋다고 평가되며, 북한의 사이버 활용도가 미미하여 공격당할 여지가 없다는 점에서 비대칭전력으로서 가장 잘 활용하고 있는 면에서는 세계 1위라 할 수 있음

□ 국내 청소년들, 사이버 메니아들이 목적 없이 장난삼아 사이버 공격을 하고 있는데 그에 대한 대비는 어떻게 하고 있는지?

⇒ 경찰의 대응 능력도 향상되고 검거율도 증가 중임. 특히 우리나라

의 청소년들의 게임 등도 포함한 수준 높은 사이버 기술을 메니아적으로 갖고 있는 부분들을 양성화시켜 우리의 역량으로 가져갈 수 있는 방안에 대한 고민이 필요함

□ 보안을 위한 집단지성 측면에서 소프트웨어 인재들이 많이 양성되어야 하는데 교육과정은 현재 어떻게 되고 있고, 어떤 것이 필요한지?

⇒ 현재 이러한 교육과정은 없으며, 중학교부터 우리도 체계적으로 필요한가 생각해 볼 때 해킹하는 친구들을 보면 교육을 통해 해킹실력이 느는 게 아니라 매니아적 기질들이 있음. 정규교과과정에 소프트웨어 교육은 가능하지만, 해커양성은 현실적으로 어려움

⇒ 문제는 현재 뛰어난 아이들이 있어도 드러날 수 없는 체계임. 매니아적 기질로 뛰어난 친구들이 대부분 공부를 못하기 때문에 현재 우리 교육체계 하에서 진로가 막혀있음. 어느 한 분야의 뛰어난 친구들이 앞으로 펼쳐나갈 수 있는 기회를 줘야하며, 아이들의 무대와 놀이터를 만들어줘야 함

⇒ 이러한 창의적인 인재양성에 있어서 '잉여'시간이 필요하고, 아무도 방향을 모르기 때문에 가르칠 수 없는데 현재처럼 부모, 교사들의 통제, 지도 하에서 학교와 학원에 갇혀 있는 환경에서는 불가능함

⇒ 수학이나 컴퓨터 구조 이해 등의 기초역량이 있는 해커는 그것이 없고 스킬만 있는 해커가 도달할 수 없는 실력의 차이. 이러한 기초역량 강화는 공교육에서 가능하며 특히 윤리 교육을 통해 무엇이 올바른 행위이며, 해당 기술로 무엇을 할 것인지 해서는 안 되는지 윤리의식을 함양시켜야 함. 스펙을 갖추지 않았더라도 기술과 윤리를 갖췄을 때 이들이 사회로 나올 수 있는 통로를 제공해줘야 함

□ 현재 우리나라의 개인정보보호가 과해 빅데이터 활용 부분에 장애가 있다는 지적이 많은데 현재 상황은 어떻고 선진국 등에서는 어떤지?

⇒ 빅데이터에서 개인정보가 담긴 것을 제외하면 건질 것이 거의 없으며 우리나라의 개인정보보호 체계는 꼭 필요한 이상의 과한 규제로 인식되고 있는 측면이 많은 것이 사실임. 선진국은 법적 개인정보 보호 체계는 우리보다도 엄격하지만 실제로는 융통성있게 활용할 수 있도록 제도가 마련되어 있음. 개인정보가 다른 정보들과 쉽게 결합되어 다 개인정보가 되는데 노이즈를 넣거나 비식별화할 방안