제 14 장
정보보호 최신동향

박 종 혁 교수

Tel: 970-6702

Email: jhpark1@seoultech.ac.kr

1.인공지능 보안
2. 5G 보안
3. 차세대보안
4. 2020년 보안 전망
5. 가트너, 2020년 10대 전략 기술 공개

1.인공지능 보안

- 인공지능을 활용한 대표적인 보안위협

속성	주요 내용
적대적 스티커 (Adversarial Patch)	- 컴퓨터가 인지하지 못하는 이미지를 담은 스티커로, 단순히 출력해서 사물 옆에만 놓아두면 이미지를 인식하는 인공지능 알고리즘이 오작동 - 자율주행차에 적용한 인공지능에 문제 발생 시 생명과 직결되는 사고가 발생할 가능성이 큼
스피어 피싱 (Spear phishing)	- 공격자가 사전에 공격 목표 관련된 정보를 수집·분석하여 공격을 수행하는 형태 - 기존 피싱(Phishing)은 숙련된 작업자가 필요했지만 인공지능을 활용하면 공격에 사용되는 숙련도가 낮아져 공격 범위 확대 가능
모방 및 흉내	- 인간의 목소리를 흉내 내지 못하지만 알고리즘을 활용하여 음성모방이 가능하며, 합성기술로 사칭 및 허위사실 유포 가능 - 인공지능은 인식하지만 사람은 해독하지 못하는 백색 소음의 명령을 음성인식시스템에 들려줌으로서 은밀하게 해킹 명령을 지시 - 딥페이크(Deepfake) 기술(Deep learning+Fake) 등을 활용하여 가짜뉴스 등을 만들어 사회 불안에 활용가능하며 영상의 진위를 가리기가 점점 어려워지고 있음
사회공학적(social engineering) 공격 자동화	- 인간이 가지고 있는 취약점을 공략하는 공격기법으로 대상자가 흥미를 가질만한 메일 링크 등을 자동 생성하여 메시지를 보내는 방법을 대량으로 자동화 및 관리
정교하고 자동화된 스웜(swarm) 공격	- 각종 취약점 및 액세스 포인트, 장치를 공격하는 스웜은 해커의 명령만 받는 봇넷과 달리 자가 학습하고, 서로 정보를 교환하면서 다수의 피해자를 공격하고 대응을 완화
인공지능 시스템의 블랙박스 모델 추출	- 블랙박스 모델의 매개변수를 추출하여 악의적 사용자가 기본 기술에 접근 가능
개인정보 유출	- 최신 디지털 정보기기들은 인공지능 기술이 탑재되어 운용되고 있으나, 이때 수집된 데이터는 사용자 동의 없이 사용되고 있어 악용 가능성 내재

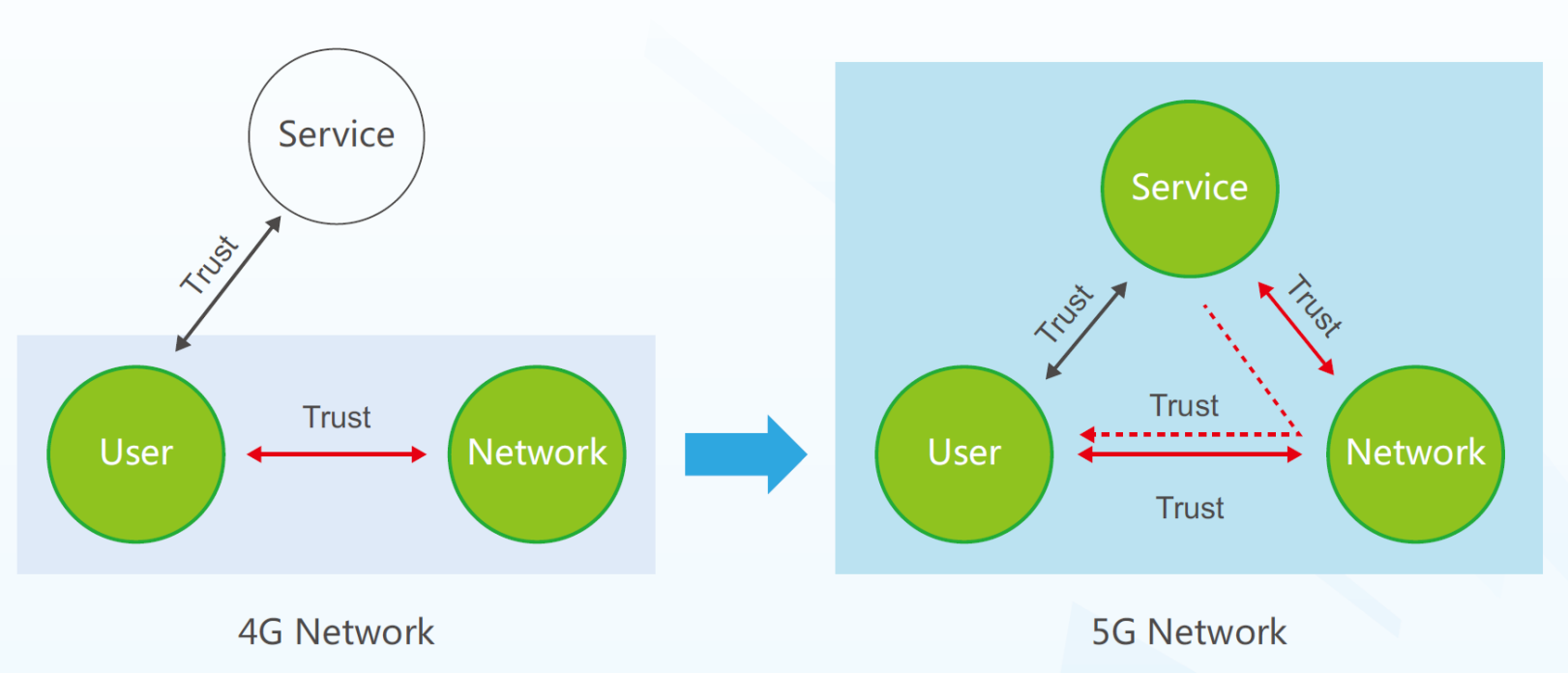
- 보안 패러다임 변화에 따른 보안 관제 주요 전략

구분	주요 내용
1세대: 단위 보안관제 (Perimeter Security)	- 방화벽, 침입탐지시스템 등 네트워크 기반 보안장비들을 활용한 초기 구축단계 - 보안 인프라의 고도화 및 안정화 단계
2세대: 통합 보안관제 (Data Security)	- 정보공유분석센터(ISAC), 종합분석시스템 등을 구축 - 위협 트래픽 관리, 취약점 관리, 웹 변조 모니터링 등 관제의 범위 확대
3세대: 빅데이터 보안관제 (Trust Security)	- 사이버위협의 고도화·지능화 - 비즈니스 환경에서 발생하는 대다수의 로그, 이벤트, 네트워크, 웹 변조 모니터링 등 관제의 범위 확대
4세대: 인공지능 보안관제 (Zero Trust)	- SOAR(Security Orchestration Automation and Response) - 머신러닝(Machine Learning based Data Analysis)

2. 5G Security

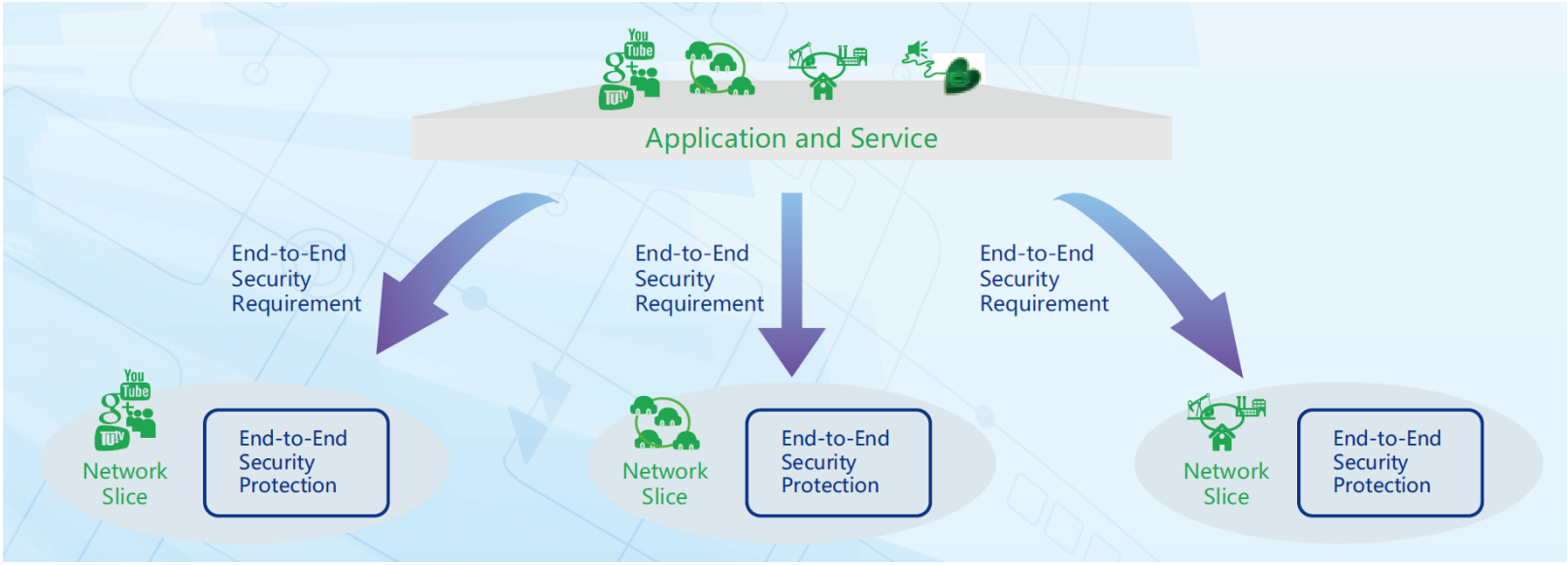
- Security Challenges Ahead of 5G
  - New Business Models
  - IT-Driven Network Architecture
    - Virtualization and Software Defined Network (SDN)
    - Network Functions Virtualization (NFV)
  - Heterogeneous Access
    - WiFi and LTE, multi-network environment – D2D Communications
  - Privacy Protection

- 5G Security 전망
  - New Trust Model and Identity Management



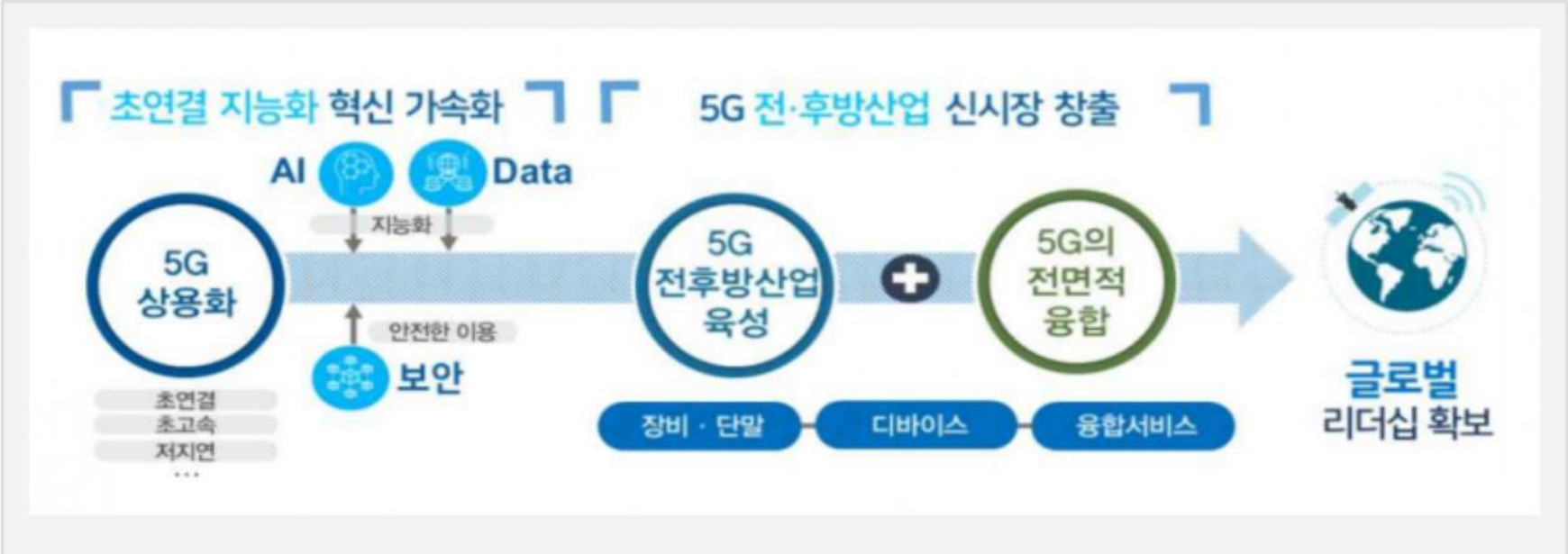
  - Hybrid Authentication Management

- A Uniformed security management framework for multi-vendor environment
  - E2E security protection



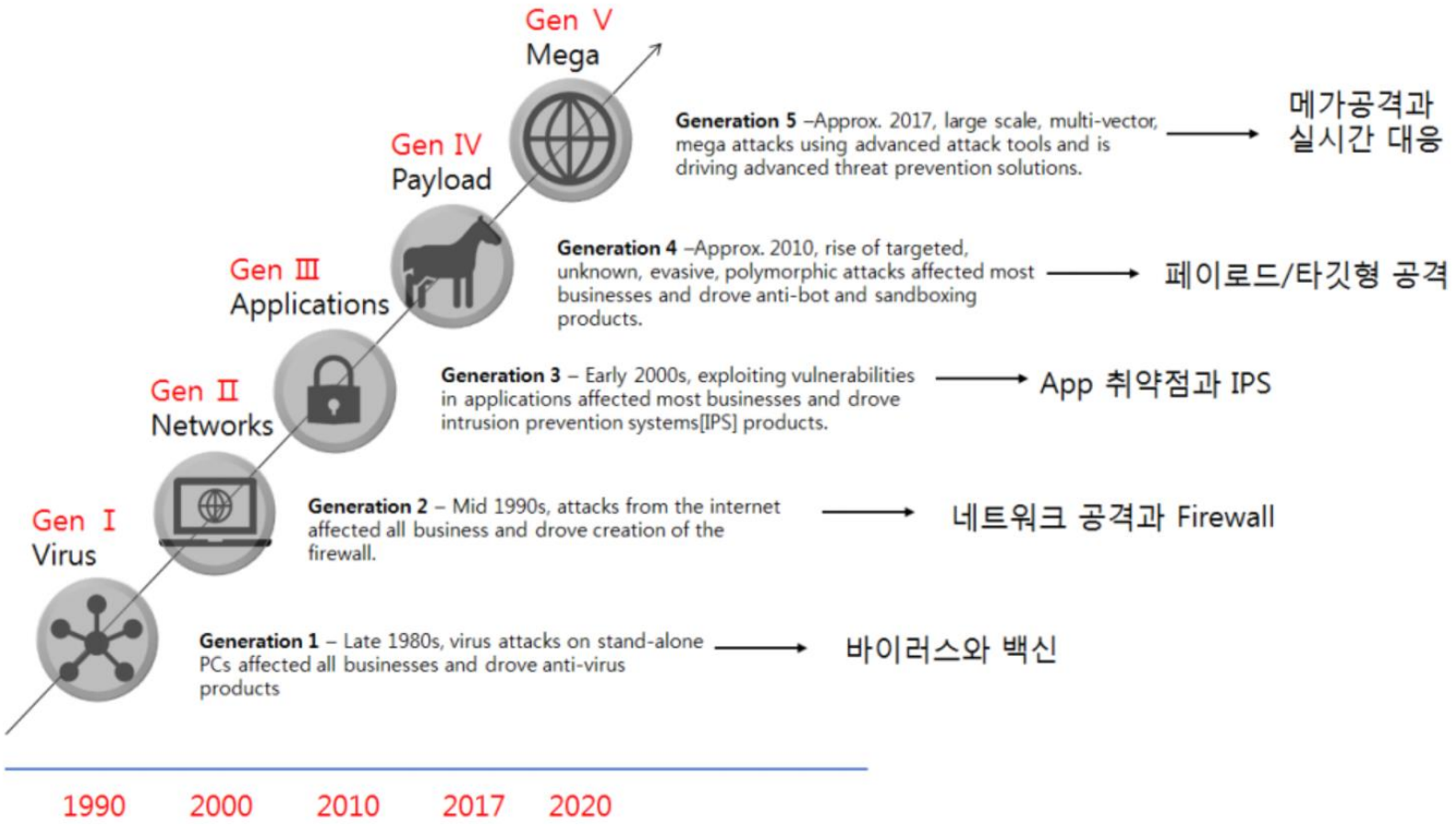
정부 5G 플러스 전략 - 정보보안 등

- 정부 5G 플러스 추진전략

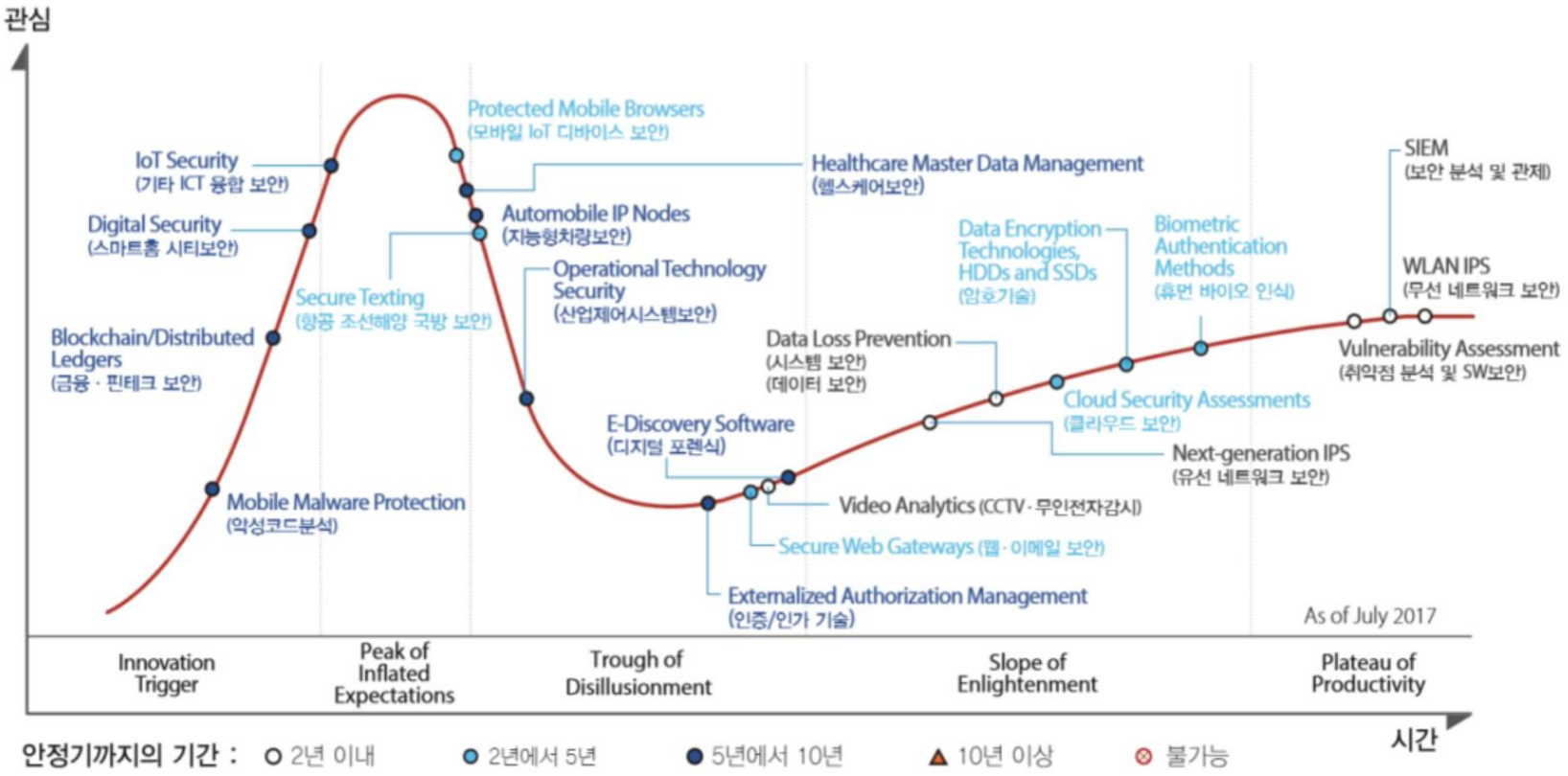


3.차세대보안

- 사이버공격의 진화



- 차세대 사이버보안 기술 예측 (by국내 전문가)



〈자료〉 IITP, ICT 기술수준조사보고서, 2018. 5.

*기술예측 정리

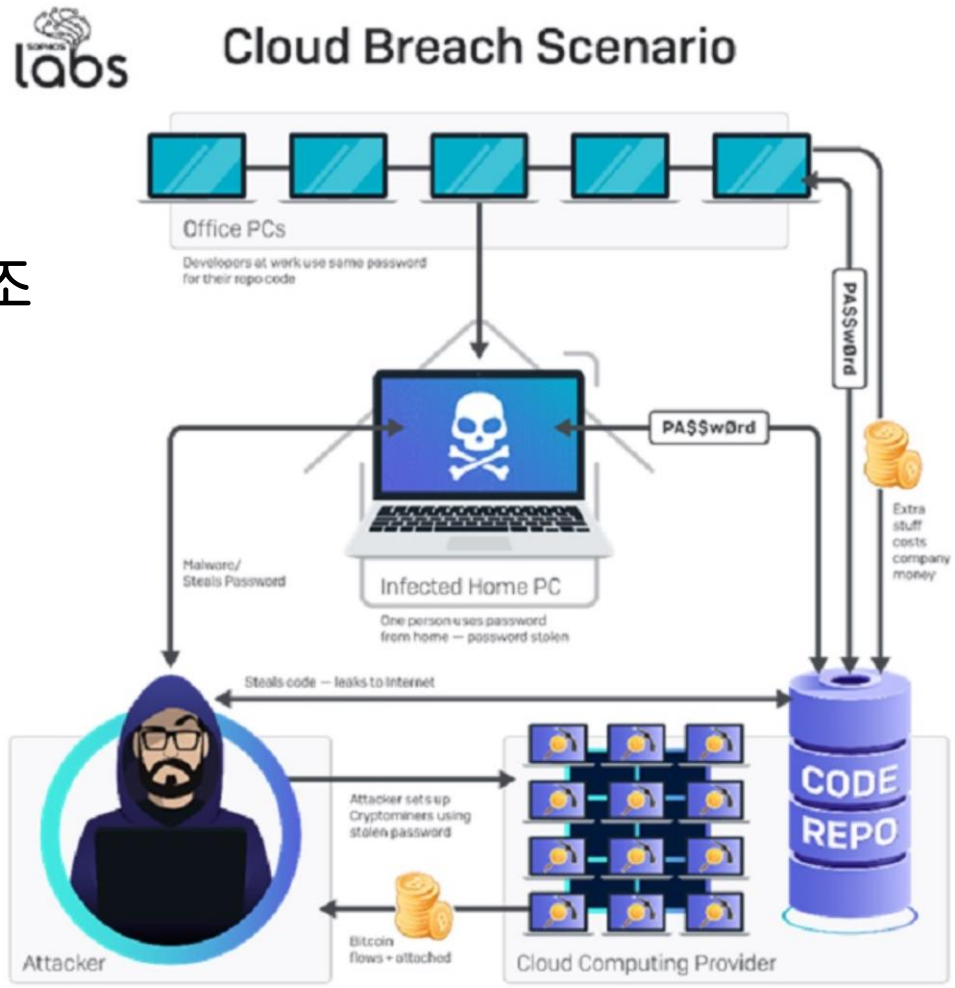
- IT 영역 – 사이버 공격기술의 진화와 대규모 사이버 공격에 대비
  - 악성 웹사이트 탐지, 멀웨어 감염탐지, 봇 프로파일링, 도메인 평가 기술 고도화 중점

- IoT/OT 영역 – 인증/인가, 보안 프레임 관리, 탐지/대응기술

- 중요정보통신시설 영역– 대규모/복합연동 시스템화가 진전됨
  - 기술의 범용화, 오픈화, 신기술 적용 트렌드를 수용하는 리스크 관리기술

4. 2020년 보안 전망

- 악성 안드로이드 앱 침투 / 클라우드 환경설정 오류 활용
  ➔ 머신러닝 역 이용 등
- 강력한 랜섬웨어 공격 집중 조



사이버위협 분야의 예상되는 구체적 문제들 (2020)

1. 랜섬웨어 공격자들

→자동화된 능동형 공격을 통해 지속적으로 공격을 강화

2. 원치 않는 앱들은 멀웨어에 가까워짐

무료체험 앱 → 차후에도 계속 사용

3. 클라우드 컴퓨팅의 최대 취약점: 운영자들의 환경설정

→ 일반적인 가시성 부족과 결합: 클라우드 컴퓨팅 환경을 사이버공격의 준비된 표적

4. 멀웨어를 막기 위해 개발된 머신러닝 자체가 공격

5. 인터넷 스캐닝의 광범위한 노이즈 속에 숨어있는 사이버범죄자의 스파이 코드를 포착하는 데 실패로 인한 위험

6. 원격 데스크탑 프로토콜(RDP)을 향한 지속적인 공격

7.자동화 능동형 공격(AAA)의 발전 추세

5. 가트너, 2020년 10대 전략 기술 공개

- **인간을 기술 전략의 중심에 두는 것은 기술의 가장 중요한 일면을 강조**
  - 기술이 소비자, 직원, 비즈니스 파트너, 사회 그리고 기타 구성원들에게 어떻게 영향을 미치는지를 잘 보여주는 것
  - 조직의 모든 행위는 기술이 개개인들과 집단에 직간접적으로 영향을 주는 방식에 기인 ➔ 인간 중심적 접근 방식
    사람, 프로세스, 서비스, 사물 등 다양한 요소들이 스마트 공간에 모여 더욱 몰입적이고 상호적이며 자동화된 경험을 창출

가트너, 2020년 10대 전략 기술 공개

- 인공지능 보안(AI Security)
  - 인공지능과 머신러닝은 다양한 사용 사례에 걸쳐 인간의 의사결정을 향상시키는 데 지속적으로 활용
  - 초자동화를 구현하는 수많은 기회를 만들어내고 자율 사물을 활용해 비즈니스 전환을 이뤄낼 수 있지만,
  - 보안 팀과 위험 분야 리더들에게는 새로운 중요 과제를 제시

➔

1. IoT, 클라우드 컴퓨팅, 마이크로서비스 및 스마트 공간 내 고도로 연결된 시스템들 ➔ 공격 가능한 포인트가 광범위

2. AI 기반 시스템 보호, AI를 활용한 보안 방어 향상, 공격자의 범죄 목적 AI 사용 예측 등 세가지 주요 영역에 초점

참고문헌

- 국경완, 공병철, “인공지능을 활용한 보안기술 개발 동향”,주간 기술동향,정보통신기회평가원, 2019
- 5G Security: Forward Thinking Huawei White Paper, 2019
- 과학기술정보통신부, “5세대(G) 플러스 전략 10대 핵심 산업과 5대 핵심 서비스”, 2019
- 이대성, “차세대 사이버보안 기술 동향”, 정보통신기회평가원, 2019
- 소포스, ‘2020년 보안 위협 전망 보고서’ 발표, 2019, 데일리시큐
- 가트너가 발표한 2020년 기업들이 주목해야 할 ‘10대 전략 기술 트렌드, 2019, 인더스트리뉴스