JKIICE

Short Paper

한국정보통신학회논문지 Vol. 23, No. 11: 1478~1481, Nov. 2019

차세대 사이버 보안 동향

The Trends of Next Generation Cyber Security

Daesung Lee[1*]

[1*]Associate Professor, Department of Computer Engineering, Catholic University of Pusan, Busan, 46252 Korea

ABSTRACT

As core technologies(IoT, 5G, Cloud, Bigdata, AI etc) leading the Fourth Industrial Revolution promote smart convergence across the national socio-economic infrastructure, the threat of new forms of cyber attacks is increasing and the possibility of massive damage is also increasing. Reflecting this trend, cyber security is expanding from simple information protection to CPS(Cyber Physical System) protection that combines safety and security that implements hyper-connectivity and ultra-reliability. This study introduces the recent evolution of cyber attacks and looks at the next generation cyber security technologies based on the conceptual changes of cyber security technologies such as SOAR(Security Orchestration, Automation and Response) and Zero Trust.

Keywords : CPS(Cyber Physical System), Next Generation Cyber Security, SOAR, Zero Trust

Ⅰ. 서 론

IoT, 클라우드 컴퓨팅, 빅데이터, 5G, 인공지능(AI) 등 4차 산업 핵심기술의 실용화로 인하여 사이버 공간과 현실 공간이 빠르게 융합되고 있는 가운데, 새로운 형태의 사이버 공격에 대한 위협도 함께 증대되고 있으며, 대규모 피해의 가능성도 점차 높아지고 있다. 특히, IoT와 더불어 드론, 자율주행차 등에 대한 사이버 공격의 가능성은 기존 사이버 보안 영역인 정보 훼손, 유출, 서비스 방해 등의 범위를 뛰어넘어 인명과 재산의 안전을 보장해야 하는 영역까지 확대되고 있으며, LTE보다 수십 배 빠른 초고속을 구현한 5G의 상용화로 인하여 초연결, 초신뢰 및 방대한 용량의 동시접속 시에 필요한 초저지연 보안기술의 구현을 필요로 하고 있다[1, 2].

따라서, 본 연구에서는 4차 산업혁명 시대의 핵심 키워드인 CPS(Cyber Physical System)의 포괄적인 안전·신뢰성 확보 및 리질리언스(resilience) 구현을 목표로 하는 차세대 사이버 보안기술과 관련된 보안 개념의 변화와 사이버 보안 핵심기술들의 연구개발 동향을 살펴보기로 한다.

Ⅱ. 사이버 공격 동향 분석

최근 5년간 RSA 컨퍼런스가 선정한 10대 키워드 추세를 분석해 보면 2016년을 기점으로 하여 APT 공격으로부터 IoT 보안, 랜섬웨어, Devops, GDPR로 보안 이슈가 이동됨을 알 수 있다[그림1].

2015	2016	2017	2018	2019
BYOD	IoT	IoT	IoT	IoT
IoT	threat actors	ransomware	ransomware	GDPR
security analytics	BYOD	devops	GDPR	blockchain
threat actors	security analytics	threat actors	iot devices	devops
home depot	kill chain	kill chain	devops	devsecops
snowden	devops	GDPR	blockchain	ransomware
software-defined	OPM	blockchain	equifax	artifical intelligence
data science	software-defined	cyber insurance	wannacry	cryptocurrency
devops	NIST CSF	security analytics	threat hunting	digital transformation
heartbleed	iot security	NIST CSF	bitcoin	women
kill chain	anthem	dark web	deep learning	containers
ransomware	dark web	bitcoin	devsecops	consumer privacy

Fig. 1 RSAC Security Issues Yearly(2015~2019)

첫째, IoT 보안은 2016년 이후 계속 주목을 받고 있는 사이버 보안의 최고 이슈이다. IoT 보안체계는 IoT 시스템의 구성에 따라 디바이스 보안, 게이트웨이 보안, 서버 보안 및 이들로 구성된 IoT 인프라 보안으로 구성되기 때문에, 사이버보안의 영역이 매우 넓으며, 이로 인

Received 31 August 2019, **Revised** 30 September 2019, **Accepted** 8 October 2019

Open Access http://doi.org/10.6109/jkiice.2019.23.11.1478 print ISSN: 2234-4772 online ISSN: 2288-4165

해 사이버 공격의 가능성도 가장 크다. 2016년 10월에 발생한 미라이(Mirai) 악성코드는 IoT 기기로 봇넷을 만들 수 있도록 해주는 악성코드를 통해 DDoS 공격을 감행한 사례이다.

둘째, 러시아에서 처음으로 유행하던 랜섬웨어(Ransomware)는 암호화 기반의 공격으로, 2013년 금품 지불을 위해 비트코인(Bitcoin) 디지털 통화를 사용하는 CryptoLocker가 출현하고, 2014년 Synology의 국가안보국(NSA)를 대상으로 하는 SynoLocker 등의 전파로 랜섬웨어에 의한 피해가 급증하였다. 또한 2017년 5월 12일에 발생한 워너크라이(WannaCry)는 해커들이 NSA에서 탈취한 해킹 툴을 활용하여 유포 하룻만에 전 세계 100여개국 10여만대 이상의 컴퓨터를 감염시켜 사상최대 규모의 랜섬웨어 피해를 유발하였다. 랜섬웨어는 앞으로도 변종 공격과 공격대상의 광범위화를 통해 공격패턴이 더욱 지능화할 것으로 전망된다.

셋째, 기업경영을 위한 IT 인프라에 다양한 보안 솔루션과 복잡한 업무시스템이 운용되면서 Devops 등 외부 협력업체가 내부망을 경유하는 경우가 급증하고 있다. 이를 이용하여 사용자에게 전달되는 소프트웨어나 하드웨어를 변조하는 공급망 공격(Supply Chain Attack)이 증가하고 있다. 2017년 6월 우크라이나에서 회계프로그램 업데이트 서버를 변조하여 랜섬웨어를 감염시키는 낫페트야(NotPetya) 공격으로 많은 기업들이 피해를 당한 것으로 보고되었다.

넷째, EU가 2018년 5월 25일부터 개인정보보호 법령인 GDPR(General Data Protection Regulation)을 시행하여 역내에서 사업장을 운영하는 기업과 전자상거래 등을 통해 해외에서 EU 주민의 개인정보를 처리하는 외국 기업들에게도 이를 적용하기로 하였다. GDPR에서는 적법성, 공정성, 투명성의 원칙, 목적 제한의 원칙, 개인정보처리의 최소화, 정확성의 원칙, 보관기간 제한의 원칙, 무결성 및 기밀성, 책임성의 개인정보보호 기본원칙을 적용하며, 이 법령을 위반할 경우에는 과징금 등 행정처분은 물론 기업 신뢰에도 영향을 미칠 수 있으므로 이 법에 위반되지 않도록 충분한 검토가 필요하다. 특히 개인정보책임자 지정 등 기업의 책임성을 강화하는 내용과 정보이동권 등 정보주체의 권리를 강화하는 내용이 추가됨에 따라 이에 대한 대응이 요구된다[3].

한편, 지난 10여년간 사이버 보안기술은 제로데이(Zero day) 공격이나 APT 공격을 방어하기 위한 안티봇(anti-bot)이나 악성코드를 탐지하는 샌드박스(Sand box) 개발을 중심으로 적극적으로 사이버 공격방어기술을 개발하여 보급하여 왔다. 하지만 최근에는 국내외에서 IP 카메라 해킹, 랜섬웨어, 가상통화 취급업소 공격, 전파 송신기를 활용한 자동차 해킹 등 새로운 형태의 사이버 사고 발생이 보고되고 있다.

Ⅲ. 사이버 보안 기술 개발 동향

정보통신기획평가원(IITP)에 따르면, 2018년 기준으로 국가별 사이버 보안기술 수준은 미국을 100%로 할 때, EU 89.7%, 한국 85.5%, 일본 83.2%, 중국 81.2%의 순으로 측정하였으며, 우리나라의 사이버 보안 기술수준은 기초, 응용, 상용화 단계에서 비슷하게 14.5%의 격차를 보이고 있는 것으로 평가되고 있다.

체크포인트는 지난 30여년간 발생한 사이버 보안사고의 시대별 변화를 기준으로 [그림 2]와 같이 2017년 4월에 발생한 워너크라이(WannaCry) 공격을 경계로 하여 현재 시점을 4세대 보안시기를 지나 5세대 보안시기로 정의하고 있다[4].

이는 기존에 이메일 첨부파일을 통해 유포시키는 일반적인 랜섬웨어와는 달리, MS 윈도우의 파일공유에 사용되는 서버 메시지 블록(SMB) 원격코드의 취약점을 악용하여, 인터넷 네트워크에 접속만 해도 감염되는 방법을 취함으로써 기존의 침입기술을 보다 지능화하면서 암호화 기법을 사용하였기 때문인 것으로 판단된다.

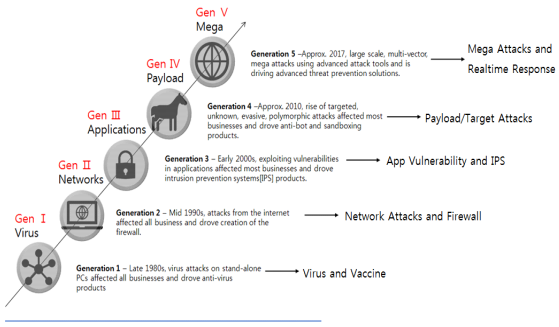

Fig. 2 Generation Evolution and Features of Cyber Security Technology

따라서 차세대 보안기술 개발의 중심은 초연결 IT 시스템의 취약점에 대한 메가공격(Mega attack)과 실시간

대응이 차세대 기술개발의 핵심을 이룰 것으로 보이며, 시스템에 접속하고자 하는 모든 사물에 접속 권한을 부여하기 전에 ID 확인 과정을 거치는 Zero Trust나 SOAR의 개념 구현이 5세대 사이버 보안 기술개발의 중심이 될 것으로 전망된다.

또한, 앞으로 4세대 보안까지 주류를 이루었던 보안장비 중심의 기술 개발로부터 딥러닝 등 AI 관련 기법을 활용하여 공격자의 진화에 예방적으로 대응하는 지능방어(Predictive Intelligence), 정상행위의 자동학습을 통해 비정상 행위를 탐지하는 행태분석탐지(Behavioral Analytics/Anomaly Detection), 엔드포인트의 대용량 트래픽을 보호 처리하는 자동 보안(Automated Security), 변종 바이러스와 좀비에 대응하는 디셉션 보안(Deception Security), 리스크가 적은 불필요한 데이터를 자동 삭제하는 Dark Data 식별기술 등이 차세대 보안기술 개발의 주류를 형성할 것으로 예측된다.

특히, 국가 차원에서는 사회혼란을 조성하거나 국가기밀을 탈취하기 위해 조직적/의도적으로 시도되는 사이버 공격의 진화에 대비하여 공격단계별로 가해지는 위협요소를 사전에 차단하는 이른바 사이버 타격순환 개념인 사이버 킬 체인(Cyber Kill Chain) 기술과 보안 supply chain에 대한 보안성 등급 평가기술(Security Rating Services: SRS)도 활발하게 연구될 것으로 보인다.

차세대 보안 기술을 추정하려는 경우, [그림 3]과 같이 미국 가트너사가 개발한 하이프 사이클(Hype Cycle)을 활용하는 것이 유용하다. 이 사이클은 기술 촉발(Technology Trigger), 기대의 정점(Peak of Inflated Expectations), 환멸(Trough of Disillusionment), 계몽(Slope of Enlightenment), 생산성 안정(Plateau of Productivity)의 5단계로 구성되며, 차세대 보안기술 영역은 주로 1단계인 기술촉발 단계에서 예측할 수 있다[5].

가트너는 사이버 위험관리를 기준으로 하여 Chaos Engineering, Digital Risk Management, Blockchain for Data Security, Design Thinking, Integrated Risk Management, IoT Security, Privacy Impact Assessments, Data Classification, Digital Ethics, File Analysis를 1단계 보안기술로 예측하고, 2단계 기술로는 Security Rating Services, Data and Analytics Governance, Bimodal IT Operation, Privacy by Design, Predictive Analysis로 예상하고 있다.

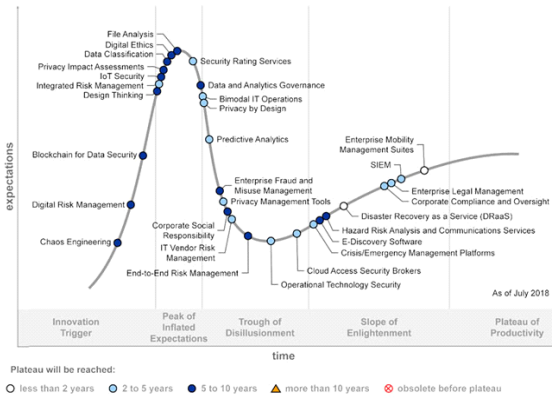

Fig. 3 Gartner's Next Generation Security Technologies Forecast Based on Risk Management

이를 토대로 국내 보안전문가들이 사이버보안 기술 관점에서 작성한 하이프 사이클에서는 [그림 4]와 같이 Blockchain for Data Security, Digital Security, IoT Security, Mobile Malware Protection의 4개 기술로 압축시킨 것이 대조를 이룬다[6].

위 자료들을 분석해 본 결과 IT 영역에서는 사이버 공격기술의 진화와 대규모 사이버 공격에 대비하여 악성웹사이트 탐지, 멀웨어 감염탐지, 봇 프로파일링, 도메인 평가 기술 고도화에 중점이 두어지고 있으며, IoT/OT 영역에서는 인증/인가, 보안 프레임 관리, 탐지/대응기술, 그리고 중요정보통신시설 영역에서는 대규모/복합 연동 시스템화가 진전됨에 따라 기술의 범용화, 오픈화, 신기술 적용 트렌드를 수용하는 리스크 관리기술이 차세대 보안기술의 주류가 될 것으로 보인다.

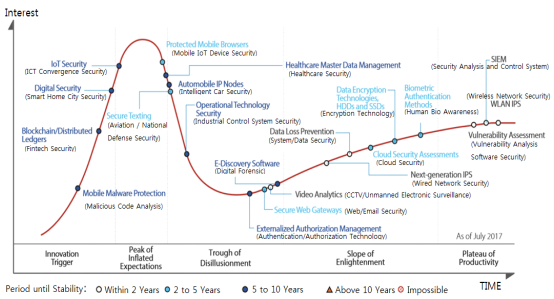

Fig. 4 Prediction of Next Generation Cyber Security Technology by IITP Security Experts

Ⅳ. 결 론

차세대 보안기술은 대용량 초고속의 트래픽을 유발하는 IoT와 5G로 구성된 초연결 CPS 인프라에 대한 초신뢰를 실시간 대응하는 방향으로 나아가고 있다. 특히, 사이버 공격자들이 AI 기반의 자동화 도구를 사용하여 메가 공격을 할 것이 예상 되므로, 방어자 측면에서도 AI 기반의 실시간 대응이 필수적이다. 이를 위해 AI 기반의 위협정보 빅데이터 수집, 처리, 분석기능을 자동화하고 실시간 모니터링과 리포팅 체계를 구현하는 SOAR와 새로운 경량 암호인증에 의한 화이트리스트기반의 Zero Trust를 구현하는 기술이 주류를 형성할 것으로 전망된다.

이러한 사이버 보안기술의 차세대 발전방향은 사이버보안 엔지니어들에게는 기밀성, 무결성, 가용성 보장이라는 기존 사이버보안 기술영역을 넘어선 것이므로 머신러닝이나 딥러닝과 같은 AI/빅데이터 기술역량을 대폭 강화해야할 것으로 판단된다[7].

ACKNOWLEDGEMENT

This paper was supported by RESEARCH FUND offered from Catholic University of Pusan(2018)

REFERENCES

[1] Telecommunications Technology Association, “Next Generation Security,” in ICT Standardization Strategic Map, pp. 305-313.

[2] Institute of Information & Communications Technology Planning & Evaluation, “Intelligent Car Security Threats and Countermeasures Report,” pp. 28-30, 2017.

[3] Korea Internet & Security Agency. [Internet]. Available: https://www.kisa.or.kr/business/gdpr/gdpr_tab1.jsp.

[4] Check Point. “Step Up to Gen V Cyber Security,” [Internet]. Available: https://www.checkpoint.com, 2019.

[5] Gartner, “Hype Cycle for Risk Management,” [Internet]. Available: https://www.gartner.com, 2018.

[6] Institute of Information & Communications Technology Planning & Evaluation, “ICT Technology Level Survey Report,” pp. 154-155, pp.167-174, 2018.

[7] D. S. Lee, “The Trends of Next Generation Cyber Security Technology,” in Weekly ICT Trends, Institute of Information & Communications Technology Planning & Evaluation Pub., pp. 2-15, 2019.