보안메트릭과 사이버 내성에 대한 연구동향분석에 관한연구

이 수 진*, 안 성 진**

요 약

오늘날 새롭게 등장한 Science of Security (SoS)라는 분야는 사이버 보안 영역에 대한 과학적인 접근 방법을 적용한 연구 분야로서 보안 영역에서 등장한 새로운 패러다임이라고 할 수 있다. 복잡하고, 큰 규모 네트워크 환경의 동적인 변화와 다수의 프로토콜과 메커니즘 환경이 존재하는 현대에 이러한 네트워크 환경에 대한 보안을 위해 Formal Model과 자동화 분야를 연구하는 방향이다. 따라서 본 연구에서는 SoS와 같은 최신 사이버 보안 연구 동향에 대해서 분석하고, 선진국들의 연구 동향 사례들을 조사하여 국내의 사이버 보안 개발 방향에 대해 새로운 접근 방법을 검토하고자 한다. 또한 다양한 사이버 보안의 패러다임에 대한 과학적 보안 연구 방법에 대해 국내의 현황을 분석해 보고 국내 사이버 보안 활성화에 대한 방향을 제시하고자 한다.

A Study on Security Metrics and Research Trend Analysis on Cyber Resilence

Sujin Lee*, Seongjin Ahn**

ABSTRACT

The emerging field of Science of Security (SoS) is a new paradigm that emerged in the field of security as a research field that applied the scientific approach to cyber security. It is a direction to study the formal model and automation field to secure the security of such a network environment in the present that dynamic change of complex, large scale network environment and a lot of protocol and mechanism environment exists. Therefore, this study analyzes the latest cyber security research trends such as SoS and examines the research trends of advanced countries to examine a new approach to cyber security development direction in Korea. We also analyze the current state of domestic scientific research on the scientific security research methods for various cyber security paradigms and present directions for revitalizing domestic cyber security.

Key words : Security Metrics, Cyber Resilience

접수일(2018년 2월 21일), 수정일(1차: 2018년 3월 23일), 게재확정일(2018년 3월 30일)

* 성균관대학교 통계학과

** 성균관대학교 컴퓨터교육과(교신저자)

1. 서 론

오늘날 자동화·융합 등의 가치를 바탕으로 '4차 산업혁명'이라는 패러다임이 확산되고 있다. 다시 말해, 산업현장에서 정보통신기술의 발전과 확산을 바탕으로 점차적으로 고수준의 컴퓨팅 능력을 필요로 하게 되고 있다는 뜻이다. 고수준의 컴퓨팅 환경을 바탕으로 각종 산업 분야에서 정보통신기술과의 융합이 점차적으로 활성화되고 이를 바탕으로 산업 현장을 비롯한 다양한 분야에서의 발전을 이끌어내고자 하고 있다. 즉, '융합'이라는 특성이 더욱 더 강조되고 있다고 할 수 있다.

실제로 이와 같은 맥락에서 여러 기술적 발전이 있었는데, 본 연구에서는 우선적으로 사이버 물리 시스템에 대하여 들여다보고자 한다. 사이버 물리 시스템은 다양한 컴퓨터 기능들이 물리세계의 일반적인 사물들과 융합된 형태의 시스템을 지칭하는 개념으로, 이러한 사이버 물리 시스템은 기존의 임베디드 시스템을 확장한 개념이라고 볼 수 있다. 또한, 이러한 사이버 물리 시스템을 구축함으로써, 현실 세계의 다양한 물리·화학 및 기계공학적 시스템을 컴퓨터와 네트워크를 통하여 자율적·지능적으로 제어할 수 있는 것으로 알려졌다. 이에 따라 실제로 각 정부기관 및 지자체 그리고 국방, 의료, 에너지 응용 분야 등을 비롯한 다양한 분야에서 사이버 물리 시스템(Cyber Physical System, CPS)의 사용이 급증하고 있다. 즉, 정리하자면 사이버 물리 시스템의 도입을 통하여 결과적으로 각종 산업을 비롯한 여러 분야에 걸쳐 긍정적인 변화를 가져오고 있다고 볼 수 있다.

그런데, 한편으로는 이러한 사이버 물리 시스템의 보편화와 관련하여 우려되는 측면 또한 있다. 바로 사이버 물리 시스템이라는 새로운 기술적 요소의 등장으로 인하여, 이러한 새로운 기술적 요소에 대한 보안 관리의 필요성이 더욱 커졌다는 점이다.[1] 사이버 물리 시스템은 기본적으로 기존과는 다른 성격의 기술적 요소라고 볼 수 있다. 그렇기 때문에, 보안 관리 측면에서도 분명 새로운 취약점이 나타날 수 있을 것으로 생각해볼 수 있다. 이러한 점을 총체적으로 고려해볼 때, 선제적 차원에서의 적극적인 보안 관리를 위한 노력이 필요하다고 할 수 있다.

이렇듯이 새롭게 요구되는 사항에도 불구하고, 기존의 사이버 보안의 접근 방법은 충분하고 근본적인 문제 해결 방법을 제공하고 있지 못하다고 한다. 그 이유는 기본적으로 기존의 사이버 보안의 접근 방법은 단순히 시스템에 가해질 수 있는 위협 요소를 진단하고 해당 위협 요소가 피해를 유발하기 이전에 대비하기 위한 보안 관제 기술을 개발하는데 주로 중점을 두었기 때문이다. 따라서 이러한 점을 고려해볼 때, 사이버 보안 연구 분야에서도 접근 방법과 관련하여 변화를 모색할 필요가 있다는 사실을 생각해볼 수 있다.

새로운 사이버 보안 분야에서의 접근 방향을 설정하기 위해서는 구체적으로 알려진 또는 가상의 다양한 위협들에 대한 대응 방법을 연구하고, VANET 등 다양한 AD-hoc network 기반의 적용 환경이 고려되어야 한다. 그리고 이와 더불어 가장 중요한 연구 방향으로는 새로운 접근법이라 할 수 있는 과학적인 SoS(science of Security) 방향의 다양한 연구를 고려해볼 필요가 있다. SoS는 그 자체로 오늘날 사이버 보안과 관련된 각종 연구에 대해 매우 중요한 의미의 방향성을 제시해 주고 있기 때문이다.

따라서 본 연구에서는 SoS와 같은 최신 사이버 보안 연구 동향에 대해서 분석하고, 선진국들의 연구 동향 사례들을 조사하여 국내의 사이버 보안 개발 방향에 대해 새로운 접근 방법을 검토하고자 한다. 또한 다양한 사이버 보안의 패러다임에 대한 과학적 보안 연구 방법에 대해 국내의 현황을 분석해 보고 국내 사이버 보안 활성화에 대한 방향을 제시한다.

2. 연구 수행 범위 및 추진전략

2.1 연구의 수행범위

본 연구는 크게 미국과 영국을 중심으로 최신 사이버보안 연구개발 동향을 분석하는 것이다. 미국에서는 크게 "Science of Security(SoS)"와 Cyber Resilience 분야를 다룬 "SURE Project"로

나눌 수 있고, 영국은 크게 “Science of Security (SoS)”분야로 구분된다.[2] SoS는 사이버보안 영역에 대해 과학적인 접근방법을 적용하여 복잡하고 큰 규모의 네트워크 환경에 능동적으로 대응하면서 다수의 프로토콜과 메카니즘 환경이 존재하는 경우에도 적용할 수 있는 방법을 찾는 것이다. 이와 관련하여 미국·영국과 같은 선진국의 사이버 보안 연구 동향을 분석함으로써 새로운 사이버 보안 연구와 관련된 방향성 설정을 위한 기본 참고자료를 확보하고자 한다.

또한, 본 연구과제에서는 “Security Metrics”와 “Cyber Resilience”와 관련된 이슈에 대하여 중점적으로 다루고자 한다. 이 두 가지 개념은 미국 National Security Agency (NSA)에서 추진하고 있는 “Science of Security (SoS)” 연구와 관련하여 제시한 다섯 가지의 Hard Problems에 속하는 두 가지 개념으로 사이버 보안에서 중요한 개념이라고 볼 수 있다. 본 연구과제에서는 “Security Metrics”와 “Cyber Resilience” 분야에 대해서도 해당 분야의 관련 연구 동향 및 실적에 대하여 조사 분석해보고자 하였다.

2.2 연구의 추진전략 및 방법

본 연구과제에서는 과학적 접근 방법이 접목된 사이버 보안에 대하여 다루어보고자 한다. 과학적 접근 방법을 접목한 기존 사이버 보안 연구 사례로는 미국과 영국의 Science of Security (SoS)가 있는데, 본 연구과제에서는 이와 관련된 연구 동향에 대하여 분석해보고자 한다. 이와 같이 과학적 접근 방법에 대한 선진 사례를 분석함으로써 향후 클라우드 컴퓨팅·사물 인터넷과 같이 다양해질 인터넷 환경에서의 새로운 사이버 보안 패러다임을 정립하는 것을 목표로 한다. 이를 위하여 구체적으로, 우선 기존의 방어 위주의 사이버 보안 접근 방식과 관련된 현황과 문제점에 대하여 분석할 필요가 있다. 그리고 “Security Metrics”와 “Cyber Resilience”의 개념과 관련 연구 동향에 대하여 분석하고자 한다.

“Security Metrics”와 “Cyber Resilience”의 경우 미국 국가안보국(NSA, National Security Agency)에서 추진하고 있는 SoS에서 제시한 다섯 가지 보안 관련 중대 이슈 중의 두 가지로, 사이버 보안의 과학적 접근 방법 중에서 반드시 고려되어야 하는 부분이라고 할 수 있다.

위와 같은 본 연구과제의 과업을 수행하기 위해서는, 문헌 연구가 주로 이루어져야 한다. 기존의 미국과 영국의 사례와 연구 동향을 분석함으로써 향후 차세대 사이버 보안의 차세대 접근 방식과 관련하여 구체화하는 것이 본 연구과제의 최종적 목표라고 할 수 있기 때문이다.

3. 사이버보안의 과학적 접근방법(SoS)의 개요

3.1 Science of Security (SoS)의 기본 개념

기본적으로 Science of Security (SoS)는 미국과 영국에서 사이버 보안 연구와 관련하여 제기된 하나의 패러다임으로서, 사이버 보안에 대한 과학적 접근 방법을 의미한다. 구체적으로는, 과학적으로 뒷받침되고 증명된 사이버 보안 관련 연구 결과를 내놓는 것에 집중하고자 하는 패러다임이라고 할 수 있다. 이러한 SoS의 경우, 2012년 미국 국가안보국 (NSA, National Security Agency)의 추진 하에 SoS 이니셔티브가 제시되면서 시작되었다. 그 이후로, SoS는 보안 과학이란 개념의 등장과 보편화를 촉진해왔고, 이를 위해서 세 가지 목표를 제시해왔다: 기초적 연구를 위한 학술적 커뮤니티에 참여, 엄격한 과학적 원리를 개발·제시, SoS 커뮤니티의 성장을 독려하는 것이다.

또한, 미국 NSA에서는 SoS와 관련된 연구를 위하여 2016년 현재 네 군데의 Science of Security Lablets을 지원하고 있다. 이들 Lablets은 카네기 멜론 대학교, 노스 캐롤라이나 주립 대학교, 일리노이 대학교 어바나-샴페인 캠퍼스, 그리고 메릴랜드 대학교에 있다. 이들은 Science of Security와 관련하여 제시된 다섯 가지의 Hard Problems와 관련하여 연구를 수행함으로써 이와 관련된 성과를 보이고 있다. 또한, 이들 Lablet은 더욱 작은 규모의 25개의 SubLablet과의 협력을 통하여 연구를 진행하고 있고, 이를 통하여 Science of Security 분야와 관련하여 2016년에만 모

두 63개의 논문·서적을 출판했다.

SoS와 관련하여 더불어서 들여다보아야 하는 내용으로 SURE Project가 있다. SURE Project는 SecUrity and REsilience for cyber physical systems를 의미하는 것으로서, 미국 NSA에서 추진하는 SoS Initiative에 의해 지원받는 또 다른 프로젝트이다. 본 프로젝트는 명칭에서 의미하는 바를 통해 파악할 수 있다시피, Resilience 이슈와 관련된 프로젝트이다. 다시 말해, 공격자로 인하여 공격이 이루어져 시스템이 정상적으로 작동하기 어려운 상황에서도 필수적인 시스템 요소의 동작이 정상적으로 이루어질 수 있도록 하는 사이버 물리 시스템을 설계하고 개발하는 프로젝트라고 할 수 있다. 이러한 SURE 프로젝트는 밴더빌트 대학교에 의해 주로 이루어지고 있고, 매사추세츠 공과 대학교, 캘리포니아 대학교 버클리캠퍼스, 하와이 대학교의 연구자들에 의해 진행되고 있다.

3.2 Science of Security (SoS) 관련 국내외 연구동향 분석

3.2.1 SoS 관련 미국의 최신 연구동향 분석

미국에서의 사이버 보안 연구는 미국 국방부 소속의 국가안보국(National Security Agency, NSA)의 지원을 받아, 보안에서의 중요한 5가지 쟁점을 먼저 선정하고 해당 문제를 해결 혹은 개선하기 위해 과학적 문제 해결 방식의 사고(Science of Security, SoS)를 반영하여 연구하는 SoS Lablet를 구성하게 되었다. SoS Lablet은 기존 CPS-VO에서 별도로 구성이 되어, SURE Project를 진행하고 있다. 위 그룹은 단일 대학의 연구가 아닌 여러 대학들(Carnegie Mellon University, North Carolina State University, University of Illinois at Urbana-Champaign, University of Maryland)이 참여하여 SoS-Vo Site에서 프로젝트별 그룹으로 묶어 연구가 진행되고 있다. 아래 5가지의 분류가 사이버 보안의 모든 것을 반영하고 있지는 않지만, 사이버 보안 영역에서 연구가 필요하다고 판단되거나, 혹은 SoS Lablet이 주요하게 관심을 가져야 하는 분야를 선정하기 위해서 분류된 것이다.

미국에서는 과학적인 증명 방식을 적용한 SoS에 따라 System Science of Security and Resilience for Cyber-Physical System Project(SURE Project)라 불리는 그룹을 구성하여 연구를 진행하고 있다. 이 프로젝트 그룹은 설계, 구축 및 대응의 존재에 필수적인 시스템 특성을 유지할 수 있는 사이버 물리 시스템(CPS)을 보장하기 위한 기반과 도구를 개발하는 것에 목표를 두고 있다.

3.2.2 SoS 관련 국내 최신 연구동향 분석

국내에서도 2010년 무렵부터 Resilience 개념을 정보보안에도 접목시키려는 노력이 있었으며, 2016년 4월 템파에서 개최된 SC 27 회의에서도 Cyber Resilience에 한 국제표준화 작업이 많은 관심 속에서 논의되었다. 이러한 관점에서, 국내에서는 “Cyber Resilience 국제표준화 동향과 이슈”라는 논문이 발표된 바가 있다. 본 논문에서는 Cyber Resilience에 대한 개념을 정리하고, Cyber Resilience 주요 모델과 구현 과제를 기술한다. 마지막으로 Cyber Resilience 국제표준화 작업에서의 주요 이슈와 활동을 소개한다. 본 논문은 세부적으로 Cyber Resilience의 개념과 관련 모델, 앞으로의 과제, 국제표준화 이슈에 대하여 다루었다.

3.3 Science of Security (SoS)와 관련된 다섯 가지의 Hard Problems

앞서 언급하였다시피, SoS와 관련하여 미국 국가안보국 (NSA, National Security Agency)에서는 SoS Initiative를 2012년에 제시했다. 그리고 SoS Initiative를 통하여 사이버 보안과 관련한 과학적 접근 방법에 대한 연구를 진행해왔다. 또한 앞서 언급하였던 바와 같이 이와 관련하여, 세 가지의 목표를 제시했다: 기초적 연구를 위한 학술적 커뮤니티에 참여, 엄격한 과학적 원리를 개발·제시, SoS 커뮤니티의 성장을 독려하는 것이다. 또한, 이러한 노력의 성과를 평가할 수 있는 항목을 제시하고자 하였다. 이러한 취지에서 제시된 것이 바로 다섯 가지의 Hard Problems라고 할 수 있다.

다섯 가지의 Hard Problem은 사이버 보안과 관련하여 과학적 접근 방법을 모색하는 것과 관련하여 고려되어야 하는 다섯 가지의 이슈 혹은 방향성을 제시

한 것으로, 관련 분야의 연구 성과가 이와 같은 다섯 가지의 이슈와 관련하여 얼마나 진전을 보였는지를 확인하고자 하는 용도로 제시되었다. 이를 통하여 Science of Security와 관련하여 얼마나 진전이 있었는지에 대하여 들여다볼 수 있도록 하였다. 다섯 가지의 Hard Problems는 다음과 같다: “Scalability and Composability”, “Policy-Governed Secure Collaboration”, “Security-Metrics-Driven Evaluation, Design, Development, and Deployment”, “Resilient Architectures”, “Understanding and Accounting for Human Behaviors”.

이 중에 Security Metrics와 Cyber Resilience는 SoS의 근본적인 취지에 가장 잘 부합하는 것으로 보인다. 먼저 Security Metrics(보안 매트릭스)는 보안 관련 데이터를 수집, 분석, 보고를 통해 결정을 내리고, 성능과 추적을 가능하게 하는 도구이다. 매트릭스의 가장 밑단의 관리지원계층(Strong Upper-level Management Support)은 관리인, 담당자 및 예산 등의 지원이 필요함을 말한다. 한 단계 위는 실질 보안 정책절차 계층(Practical Security Policy and Procedure)인데 의미 있는 실질적인 보안정책과 절차가 필요함을 보인다. 그 위에는 정량적 성능계층(Quantifiable Performance Metrics)이 있는데 제대로 된 의미 있는 성능 데이터를 수집 분석해야 함을 말한다. 결과지향적 매트릭스 분석계층(Results-Oriented Metrics Analysis)은 정기적인 분석을 통한 교훈 섭렵과 보안제어의 향상 등이 필요하다.

다음으로 Cyber Resilience에 대한 정의는 많은 전문가에 의해 다양하게 논의되고 있지만 가장 일반적이고 보편적 인 정의는 다음과 같다. Cyber Resilience는 부정적인 사이버 이벤트에도 불구하고 의도한 성과 및 결과물을 지속적으로 전달할 수 있는 능력(ability)을 의미 한다’ 여기에서 주목할 것은 Cyber Resilience는 능력 이라는 이며 이는 정보시스템, 비즈니스 기능, 조직, 지역 또는 도시, 국가 또는 사회, 또는 국제적 수 등 다양한 차원에서의 능력을 의미할 수 있다. 지속적으로 전달한다는 것은 정상인 전달 메커니즘이 실패하였을 때, 즉 위기 상황이거나 보안사고 발생 후에도 의도한 결과물을 제공할 수 있어야 함을 의미한다. 이는 정상으로의 복구도 포함한다. 바로 이 점에서 Business Resilience와 구분을 할 수 있다. Cyber Resilience는 사고가 발생한 후 정상상태로의 조속한 복구 역량(회복력)도 중요하지만, 이를 위한 조직 내의 관련 부서(: IT 운영부서, 보안부서, BCM 부서 등)간의 업무 협조를 기반으로 조직에 악영향을 줄 수 있는 요인에도 사고가 발생하지 않도록 하고, 설령 사고가 발생해도 조속히 탐지해서 정상상태로 복귀할 수 있는 역량(면역력)을 강조하고 있다. 따라서 Cyber Resilience는 곧 ‘사이버 면역·회복력’이라고 번역하는 것을 제안한다.

Security Metrics와 Cyber Resilience는 보안과 관련된 계량화된 솔루션과 개선 방안을 제시하고 이를 바탕으로 시스템의 Resiliency를 강화함으로써, SoS 표현 자체가 내포하고 있는 “사이버보안의 과학적 접근”이라는 내용과 의미 측면에서 가장 근접하다고 보았기 때문이다.[3] 따라서 이 두 분야에 대해 중점적으로 다루겠다.

4. Security Metrics와 Cyber Resilience 연구동향 분석

본 연구과제에서는 사이버 보안과 관련된 과학적 접근 방법에 대한 연구 동향을 분석하기 위하여 우선적으로 미국 국가안보국(NSA, National Security Agency)에서 발간한 “Science of Security and Privacy Annual Report 2016”을 참고하였다. 이러한 Annual Report를 분석함으로써 최신 선진 사례의 연구동향에 대해 Security Metrics 분야와 Cyber Resilience 분야에 중점을 두며 연구 동향에 대해서도 분석해보고자 했다. 이를 위해 “Science of Security and Privacy Annual Report 2016”에 수록된 각 Lablet의 프로젝트와 관련된 정보를 기준으로, 특정 프로젝트가 Security Metrics와 Cyber Resilience 두 분야 모두에 관련되어 있다는 내용이 명시되어 있는 경우 해당 프로젝트를 분석 대상으로 선정했다. 선정된 프로젝트 일부의 논문성과에 대해 살펴보도록 하겠다.

4.1 Security Metrics·Cyber Resilience 공통 해당 분야

"Science of Security Lablets: North Carolina State University"에서는 Attack Surface and Defense-in-Depth Metrics프로젝트를 수행하였다. 본 프로젝트를 통한 가장 중요한 기술적 성과는 stack traces를 사용하여 attack surface를 매핑한 것이다. Attack Surface 데이터가 충돌이 발생하고 stacktraces가 보고한 바이너리 값에서의 취약점을 예상하는데 사용될 수 있음을 보여주었다. 또한, 메소드 레벨에서의 취약점을 예측하기 위한 콜 그래프에 대한 Random Walk를 사용하는 예측 모델을 개발하였다.

논문성과는 "NANE: Identifying Misuse Cases Using Temporal Norm Enactments"[4]인데, 합법적인 사용자의 오용으로 인한 데이터 기밀성의 침해는 기존의 Requirement Engineering으로는 탐지가 어려운 것이 사실이었다. 따라서 본 연구에서는 추론을 통하여 오용을 탐지해내는 NANE이라는 프레임워크를 제시함으로써 합법적인 사용자의 오용과 관련된 탐지를 개선하고자 하였다. 본 연구에서는 앞서 다룬 기본적인 개념을 바탕으로 Norm Enactment에 대하여 다루고 있다. 여기서 "Enactment"는 시스템에서 가능한 모든 history와 이러한 history를 구성하는 모든 events를 의미한다.

또한, 이를 바탕으로 Misuse Case를 발견해내기 위하여 NANE Framework를 제시한다. 이 과정에서 본 연구는 Sociotechnical System(STS)를 제시한다. 여기에서 STS는 stakeholder를 대표하는 "Autonomous Agents"가 기술적 요소를 통하여 상호작용하도록 되어 있는 사회적인 조직을 의미한다. 이러한 STS를 기반으로 제시된 NANE Framework을 여러 단계로 요약하였다.

본 연구에서 NANE이라는 "Temporal Reasoning Framework"를 제시함으로써 체계적으로 "Norm Enactment"를 생산하고 오용을 효과적으로 탐지할 수 있게 되었다. 이를 통해 로그를 기반으로 잠재적인 오용에 대하여 선제적인 대응을 할 수 있게 되었다. 다만, NANE은 한 시점에 한 개의 Norm만을 탐색할 수 있어서 실용적인 문제가 있을 수 있다. 따라서 추후에 이와 관련된 연구가 요구된다.

4.2 Security Metrics 분야

"Security Metrics 분야"Science of Security Lablets: University of Illinois at Urbana-Champaign"에서 수행한 프로젝트 관련 논문 성과를 살펴보도록 하겠다. Data-Driven-Model-Based Decision-Making 프로젝트를 수행했는데, 내용은 다음과 같다. 예측을 위한 Security Metrics는 시스템의 모든 측면을 고려하여야 한다. 하지만 종종 간과되고 있지만 중요한 요소가 있는데, 바로 인적 요소와 관련된 내용이다. 따라서 본 프로젝트에서는 인간의 행동과 의사결정을 고려한 HITOP 모델링을 개발했다. 각 사용자의 기회, 의지, 개개인에게 주어진 일을 수행하는 능력들을 고려함으로써 시스템의 안전한 상태를 유지하기 위한 바람직한 사용자의 역할에 대하여 다루었다. 논문성과는 "Impact of Policy Design on Workflow Resiliency Computation Time"[5]가 있으며, 요약은 다음과 같다. 작업 흐름은 어떠한 작업이 특정한 정책적 제약조건 하에서 어떠한 순서로 어떻게 이루어져야 하는지에 대하여 명시해놓은 개념이다. 다만, 이러한 작업 흐름과 관련해서 생각해볼 때 예기치 않은 여러 요소가 갑작스럽게 발생할 수 있다. 이러한 예상치 못한 변동이 발생했을 때에도 작업은 원활하게 이루어지도록 해야 할 필요가 있는데, 이를 위해서는 Workflow가 재구성되어야 할 필요성이 있다. 다만, 갑작스러운 변동으로 인한 피해를 최소화하기 위하여 여기에서 이러한 Workflow의 재구성은 빨리 이루어져야 할 필요가 있다. 이러한 관점에서, 본 연구에서는 Resiliency와 관련된 연산 시간에 주목한다. 특히, 보안 정책의 변화가 어떠한 방식으로 Resiliency를 연산해내는데 소요되는 시간을 영향을 주는지에 대하여 들여다보고자 한다.

본 연구를 통하여, Workflow와 관련된 보안 정책이 Resiliency 방안의 산출 시간에 영향을 준다는 것을 알아낼 수 있었다. 이와 관련하여, 새로운 보안 정책과 관련된 제약조건이 추가되거나 제거되는 식의 변화가 Resiliency 산출 시간에 유의미한 영향을 준다는 것이 확인되었다. 또한, 보안 정책의 변화가 Workflow의 Resiliency와 관련된 방

안을 도출해내는 연산 시간에 상당한 영향을 준다는 점을 확인해볼 수 있었다. 또한, 인위적인 보안 정책적 제약조건을 추가하는 것이 Resiliency 연산 시간을 획기적으로 단축시킨다는 점도 확인해볼 수 있었다. 이러한 점에서 볼 때, 보안 정책과 Resiliency 상의 상당한 연관성을 파악해볼 수 있다. 다만, 본 연구에서는 Cardinality, 한 사람이 작업에 투입할 수 있는 시간의 제한과 같은 복잡한 제약조건이 고려되지 않았다. 또한, 순환(Loop) 형태의 복잡한 작업 흐름이 고려되지 않았다. 따라서 본 연구 결과의 실질적 적용가능성을 높이기 위해서 이와 같은 복잡한 환경에서의 실험 및 연구도 진행되어야 할 필요성이 있다.

4.3 Cyber Resilience 분야

"Science of Secure Resilient Cyber-Physical Systems (SURE)" Project 관련 논문 성과를 살펴보겠다. SURE Project는 2014년에 시작된 것으로서, 공격자가 존재하고 있는 상황에서도 사이버 물리 시스템(CPS, Cyber-Physical System)으로 하여금 필수적인 시스템 특성을 유지할 수 있도록 설계하고 보장하는 도구와 기조를 개발하는 프로젝트이다.[6] CPS는 스마트 그리드, 트래픽 제어, 메디컬 모니터링, 자율주행 자동차와 같이 물리적 요소와 컴퓨터 요소가 밀접하게 결합된 장비를 의미한다. SURE은 미국 National Security Agency (NSA)의 재정적 지원을 받는 프로젝트로서, 사이버 물리 시스템에서의 Resiliency와 관련된 과학적 이해를 높이는 것을 목표로 하고 있다. 이 프로젝트는 상당한 수준의 자원과 의사결정의 분산화·분권화에도 불구하고 Resiliency를 확보한 시스템을 설계하는 문제에 대해서 다루고 있다. 본 연구 프로그램의 필수적인 부분은 바로 시스템 설계자와 시스템을 조작하는 사람과의 통합적·컴퓨터 기반·물리적 상호작용 현상의 맥락에서 보안과 Resilience에 대해 이해하고 편하게 사용·관리할 수 있는 새로운 기술자들을 양성해내기 위한 지속적인 노력을 기울이도록 하는 것이다. 성과논문으로는 "Optimal Thresholds for Intrusion Detection Systems"[7]가 있다. 네트워크와 사이버 물리 시스템(CPS, Cyber Physical System)과 관련하여 중요한 보안상의 위협으로 "Stealth Attack"이 있다. "Stealth Attack"은 공격자에 대한 정보가 명확하게 드러나지 않는 공격 유형을 일컫는 용어로서, 오늘날의 보안관제에 심각한 도전이 되고 있다.

이러한 "Stealth Attack"으로부터 시스템을 지키기 위해서는 여러 침입탐지시스템(IDS, Intrusion Detection System)이 갖추어져야 한다. 그런데, 여기에서 IDS는 자체적인 민감성(Sensitivity)에 따라 수많은 False-Positive/False-Negative Alarm을 발생시킨다. 이러한 False-Positive/False-Negative Alarm은 결과적으로 시스템 자원의 고갈을 불러일으키고 시스템의 성능을 저해할 뿐만이 아니라 IDS로 하여금 제대로 된 기능을 수행하기 어렵게 만든다. 더군다나, 다수의 IDS가 구축된 환경에서는 각각의 IDS마다 Sensitivity도 각기 다를 것이기 때문에 이와 관련된 문제는 더욱 심각해진다고 할 수 있다. 따라서 본 연구에서는 이러한 Sensitivity로부터 발생하는 방어자의 손실을 최소화할 수 있는 최적의 Sensitivity를 찾아주는 알고리즘을 제시하고자 한다.

침입탐지 시스템은 "Stealthy Attack"을 탐지하는데 중요한 도구이다. 이러한 맥락에서 볼 때, Detection Threshold을 조절함으로써 IDS의 Sensitivity를 최적화하는 것은 보안성을 높이고 비용을 줄이기 위해서 매우 중요하다고 할 수 있다. 따라서 본 연구에서는 Multiple IDS 환경에서의 최적화된 Detection Threshold를 도출하는 알고리즘을 게임이론을 바탕으로 제시하였다. 그 결과, 본 연구에서 제시한 알고리즘은 두 개의 Baseline 전략(Locally Optimal과 Uniform)보다 더 높은 성능을 보이는 것으로 나타났다. 향후에는 이를 바탕으로 다양한 종류의 Application 환경을 고려하기 위하여 Supermodular 혹은 Additive Function과 같은 다른 차원의 Damage Function을 고려하는 것을 목표로 할 필요가 있다. 또한, 시스템의 Application 고유의 특징을 추가적으로 고려할 필요가 있다.

5. 결 론

5.1 연구의 기대 효과

본 연구는 사이버보안시스템의 대응 방법에 대한 한계점 혹은 새로운 연구 개발 방향을 제시하여 현재의 사이버보안 근본 문제점을 해결하고자 새로운 과학적 접근 방법을 찾고 있는 개념 정립 단계의 연구이다. 따라서 미국과 영국을 중심으로 기본의 사이버 보안 시스템의 한계점을 새로운 접근 방법에 의해 연구를 진행하는 측면에서는 신기술 개발보다는 새로운 패러다임의 연구 개발 방향을 제시하고 실험적인 연구들을 진행하고 있다.

아직은 초기 단계의 연구이지만 사이버보안 분야의 선진국이라 할 수 있는 미국과 영국의 사이버보안에 대한 근본적인 문제 해결 방법을 찾고자 하는 연구 방법들을 우리도 자료수집 및 내용을 검토하여 실제 접근 방법을 연구하는 것은 매우 중요한 연구 분야이다. 향후 클라우드, 빅 데이터 그리고 사물 인터넷 등 다양한 컴퓨팅 환경 및 네트워크의 확장성은 물론 새로운 패러다임의 사이버침해 및 보안에 대한 연구들이 연계되어 새로운 사이버보안에 대한 개념 정립과 연구 방향의 제시가 필요하다. 이러한 컴퓨터 시스템 및 다양한 네트워크 환경을 고려할 경우 사이버보안에 대한 근본적인 문제 해결 방법을 고찰하는 것은 매우 의미 있는 연구 방향이라 판단된다. 특히, 본 연구 과제에서는 사이버보안의 과학적 접근 중에서도 “Security Metrics”와 “Cyber Resilience”라는 분야에 더욱 집중하였다. 미국 국가안보국에서 발간한 “SoS Annual Report 2016”에 따르면 사이버보안의 과학적 접근(SoS, Science of Security)에는 다섯 가지의 Hard Problems가 제시되어 있는데, 이 두 가지 개념은 Hard Problems의 일종이다.

본 연구에서 “Security Metrics”와 “Cyber Resilience”에 집중한 이유는 이 두 가지의 세부적인 분야가 SoS의 근본적인 취지에 가장 잘 부합한다고 보았기 때문이다. 이러한 분석 과정을 통하여 일련의 연구 동향을 파악할 수 있었고, 향후 사이버 보안의 과학적 접근과 관련된 국내의 학문적 방향성을 다시금 정립할 수 있을 것으로 기대된다.

5.2 활용방안과 추후 연구과제

5.2.1 본 연구과제의 활용방안

본 연구과제에서의 목적은 기존의 방어 위주의 소극적인 사이버 보안에서 탈피하여, 조금 더 선제적이고 적극적으로 보안 위협에 대하여 대응할 수 있도록 하는 사이버 보안의 패러다임에 대하여 정립하는 것이다. 이러한 목표를 위하여, 본 연구과제에서는 과학적 사이버 보안 접근 방식의 대표적인 사례인 Science of Security (SoS)에 대하여 다루었다. 그 가운데에서도 특히 “Security Metrics”와 “Cyber Resilience” 분야에 대한 내용을 집중적으로 조명하였다.

이와 같이 본 연구를 통하여 전반적인 관점에서는, 사이버 보안의 과학적 접근 방법과 관련하여 선진국에서는 어떠한 연구가 이루어지고 있는지에 대하여 개괄적으로 파악할 수 있을 것으로 기대된다. 따라서 본 연구과제의 분석 결과를 바탕으로 향후 새로운 과학적 접근을 바탕으로 한 사이버 보안의 패러다임과 관련하여 향후 방향성을 정립하는데 활용될 수 있을 것으로 기대한다.

5.2.2 추후 연구 과제

앞서 언급한 바와 같이, 본 연구과제에서는 “Security Metrics” 분야와 “Cyber Resilience” 분야를 중심으로 사이버 보안에 대한 과학적 접근 방식을 확립하는 것을 목표로 선진국의 관련 연구 동향을 심층 분석하고 있다. 이를 통하여, 기본적으로 새로운 패러다임인 “사이버 보안에 대한 과학적 접근 방식”에 대한 이해도를 높일 수 있을 것으로 기대되고, 이를 바탕으로 한 국내의 사이버 보안 관련 연구의 향후 방향성을 제시할 수 있을 것으로 기대된다.

다만, 아직 과학적 접근 방식의 경우 초보적 단계에 해당하므로 향후 이와 관련하여 많은 발전과 변화가 있을 것으로 예상된다. 이에 따라, 지속적으로 과학적 접근 방식과 관련된 연구 동향의 변화에 관심을 가질 필요가 있다. 지속적으로 사이버보안에서의 과학적 접근이라는 새로운 패러다임에 주목함으로써 향후 사이버 보안의 확립과 보완

및 강화를 위하여 어떠한 아이디어와 패러다임이 나타날 것인지에 대하여 시의 적절성을 잃지 않도록 추가적인 후속 분석연구가 요구될 것으로 보인다.

본 연구에서 보여준 SoS 관련 동향을 바탕으로 단순히 학문적인 방향성을 결정하는 것을 넘어서서, 해당 연구의 동향이 실질적으로 사이버 보안을 강화 발전시킬 수 있는 방향으로 나아가기 위해서는 실무적 차원에서의 노력 역시 병행되어야 한다. 따라서 이러한 점을 고려해볼 때, 향후에는 단순히 해외의 학문적 연구 동향을 분석하는 것 이상으로 실무적 차원에서의 사이버보안의 과학적 접근이라는 패러다임의 적용 방안을 고안·도출할 필요가 있다.

참고문헌

[1] Perelman, L. S., Abbas, W., Koutsoukos, X., & Amin, S. (2016). Sensor placement for fault location identification in water networks: A minimum test cover approach. Automatica, 72, 166-176.

[2] US National Security Agency, Science of Security and Privacy Annual Report 2016.

[3] Mace, J. C., Morisset, C., & Van Moorsel, A. (2015, September). Impact of policy design on workflow resiliency computation time. In International Conference on Quantitative Evaluation of Systems (pp. 244-259). Springer, Cham.

[4] Kafali, Ö., Singh, M. P., & Williams, L. (2016, September). Nane: Identifying misuse cases using temporal norm enactments. In Requirements Engineering Conference (RE), 2016 IEEE 24th International (pp. 136-145). IEEE.

[5] Mace, J. C., Morisset, C., & Van Moorsel, A. (2015, September). Impact of policy design on workflow resiliency computation time. In International Conference on Quantitative Evaluation of Systems (pp. 244-259). Springer, Cham.

[6] Laszka, A., Potteiger, B., Vorobeychik, Y., Amin, S., & Koutsoukos, X. (2016, April). Vulnerability of transportation networks to traffic-signal tampering. In Proceedings of the 7th International Conference on Cyber-Physical Systems (p. 16). IEEE Press.

[7] Laszka, A., Abbas, W., Sastry, S. S., Vorobeychik, Y., & Koutsoukos, X. (2016, April). Optimal thresholds for intrusion detection systems. In Proceedings of the Symposium and Bootcamp on the Science of Security (pp. 72-81). ACM.

〔저자소개〕

이 수 진

2012 가천대학교
응용통계학과(학사)
2016 성균관대학교
통계학과(석사)

E-Mail : rosaline@skku.edu

안 성 진

1988 성균관대학교
정보공학과(학사)
1990 성균관대학교
정보공학과(석사)
1998 성균관대학교
정보공학과(박사)
1990~1995 KIST/SERI 연구원
1996 정보통신기술사
1999~현재 성균관대학교
컴퓨터교육과 교수
관심분야 : SW교육, 정보윤리, 정보보안
E-Mail : sjahn@skku..edu