Journal of Digital Convergence
Vol. 17. No. 8, pp. 105-113, 2019
ISSN 1738-1916
https://doi.org/10.14400/JDC.2019.17.8.105

핵심기반시설 사이버 보안 평가 모델링 기법 연구

엄익채
한전KDN(주) 보안컨설팅팀 차장

A study on the cyber security assessment modeling of critical infrastructure

Ieck-Chae Euom
Deputy General Manager, Cyber Security Consulting Team, KEPCO KDN

요 약 본 연구는 원자력 발전소등의 국가 핵심기반시설에 대한 기존의 사이버 보안 위험 모델링 기법을 분석하고 이의 한계점 및 개선방안을 도출하는데 목적이 있다. 연구 대상은 전력 및 원자력 발전소, SCADA등의 국가 핵심기반시설의 사이버 보안 위험 모델링 기법이다. 연구에서는 SCADA, 전력, 원자력 발전의 사이버 보안 위험 모델링 분야의 총 26편에 대한 선행 연구 사례를 분석하고, 이를 정성적 모델링과 정량적 모델링 기법으로 구분하여 각각의 특징과 한계점에 대해 분석하였다. 최근 핵심기반시설은 디지털화 되어 가는 추세이며 Windows등의 운영체제를 사용하는 시스템들로 구성되어 있지만, 상시 운영되어야 하는 요구사항으로 인해, 취약점이 발견되더라도 패치등을 즉각 행할 수가 없는 특징이 있다. 본 연구에서는 이러한 제약사항들을 감안하여 취약점들이 핵심기반시설의 생명주기동안 어떤 특성으로 전파되고 예방 할 수 있는지에 대한 모델링 기법 방안을 제시하고 있다.

주제어 : 핵심기반시설, 위험 모델링, 취약점 생명주기, 취약점 발견모델, 공격 그래프

Abstract The purpose of this study is to analyze cyber security risk modeling of critical infrastructure, draw out limitations and improvement measures. This paper analyzed cyber security risk modeling of national critical infrastructure like as electricity sector, nuclear power plant, SCADA. This paper analyzed the 26 precedent research cases of risk modeling in electricity sector, nuclear power plant, SCADA. The latest Critical Infrastructure is digitalized and has a windows operating system. Critical Infrastructure should be operated at all times, it is not possible to patch a vulnerability even though find vulnerability. This paper suggest the advanced cyber security modeling characteristic during the life cycle of the critical infrastructure and can be prevented.

Key Words : Critical Infrastructure, Risk modeling, Vulnerability life cycle, Vulnerability detection model, Attack graph

1. 서론

핵심기반시설은 전력, 발전소 및 은행과 같은 에너지와 금융시스템 등 국가의 주체가 되는 핵심 자산을 의미한다. 전통적으로 핵심기반시설 분야인 전력설비, 화력발전소, 원자력발전소 등은 전용 통신장비와 폐쇄망의 네트워크에서 운영되었다. 그러나 최근 Windows등의 상용 운영체제와 일부 개방된 네트워크 체계가 적용되고 있으며, 이는 디지털화 되는 핵심기반시설들의 사이버 보안 위험성이 증가하여 이와 관련된 보안조치가 필요하다. 최근 정보화 사회를 위협하고 있는 '해킹'은 단순히 개인, 회사 등의 범위를 넘어서 국가의 안전을 위협할 수 있는

*Corresponding Author : Ieck-Chae Euom(icelaken@gmail.com)
Received June 28, 2019 Revised July 29, 2019
Accepted August 20, 2019 Published August 28, 2019

영향력을 나타내고 있다. 이와 관련된 최근 사례는 이란 원자력발전소에서 발생한 스턱스넷(Stuxnet)이다.스턱스넷은 2010년 6월 발견된, 지멘스의 산업기반제어시스템을 공격하는 Windows 운영체제의 웜바이러스이다. 스턱스넷은 가장 강력한 보안체계를 적용하고 유지한다고 여겨졌던 발전소, 제어시스템을 대상으로 하며 핵심기반 시설에 정밀하고 고도화된 타겟공격을 수행하여 사이버 미사일 또는 지능화된 공격이라고도 불리어진다. 최근 핵심기반시설의 계측제어시스템은 디지털화되어가고 있으며, Windows 등의 상용 운영체제가 설치된 시스템들로 구성되어 있다. 이런 상용 운영체제들의 취약점은 매일 새롭게 발견되고 있으며, 핵심기반시설의 취약점들이 발견부터 패치적용-소멸까지 생애 주기 동안 어떠한 경로로 전파되고 효과적으로 예방할 수 있는지에 대한 연구가 필요하다.

특히, 핵심기반시설은 취약점이 발견되더라도 패치를 즉시 적용할 수가 없다. 또한 인터넷과의 연결이 망 분리 등으로 단절되어 있어, 네트워크를 통한 직접적인 공격을 받을 수 없는 특징이 있다. 이러한 핵심기반시설의 특성을 고려한 제어시스템에 대한 취약점이 시간 경과에 따라 어떠한 잠재적인 영향을 가져갈 수 있는지 알아보는 사이버 보안 평가 모델링에 대한 연구가 필요하다. 이러한 사이버 보안 평가 모델링에 대한 정의는 기관에 따라 다양하게 정의를 하고 있다. 국제적인 정보보호기관인 SANS에서는 Fig. 1과 같이 보안 평가를 3단계로 구분하고 있다[1].

Fig. 1. Elements of Cyber Security Assessment

첫째, 위협 평가(threat assessment)는 자산을 목표로 하는 위협원에 대한 공격을 나타내며 해킹이나 서비스 거부 등의 공격을 나타낸다. 둘째, 취약점 평가(vulnerability assessment)는 위협을 악용하기 위한 사전 조건이나 경로를 의미한다. 평문 전송이나 익스플로잇 코드 발견, SQL인젝션, 비밀번호 노출 등이 예이다. 셋째, 위험 평가(risk assessment)는 위협원이 취약점을 악용하여 위협이라는 행위를 통해 자산에 악영향을 미치는 결과를 가져올 가능성을 나타낸다.

발전소에 존재하는 핵심기반시설에 대한 위험의 경우 예를 들면, 취약점은 핵심기반시설 내에 존재하는 악용 가능한 운영체제 취약점이 되며 위협은 사용 가능한 공격 경로를 의미한다.

2. 선행 연구 분석

선행 연구 분석에서는 핵심기반시설에 해당하는 SCADA, 미국 전력연구원, 미국 원자력협회의 26편의 선행 연구를 분석하였다.

2.1 SCADA

SCADA(Supervisory Control And Data Acquisition)시스템은 지역적으로 분산된 시스템의 감시제어와 데이터를 취득하고 관리하는 시스템을 말한다[2]. SCADA시스템은 전력, 화학, 철도 등 국가 핵심기반시설의 제어 및 감시용으로 널리 적용되고 있으며, SCADA시스템의 보안성 평가 및 조치에 관련된 다양한 선행 연구들이 진행되었다. 학술검색 사이트인 구글 스칼라(Google Scholar)에서 SCADA시스템에 대한 보안 평가 모델링 연구를 검색하면 총 24편의 논문 결과를 볼 수 있다. Table 1은 2004년부터 2018년까지 SCADA 시스템의 보안성 평가 관련 24편의 논문에서 언급하고 있는 보안 평가 모델링 기법을 보여주고 있다.

Table 1. Classification of precedent researches

Category	Ref.
scenario based modeling	[3,4,5,6,7,8,9,10,11,12]
Attack Graph	[13,14,15,16,17,18]
Attack Tree	[19,20,21,22]
Vulnerability Tree	[23]
Compromise Tree	[24]
PetriNet	[25]
CORAS	[26]

시나리오 기반 사이버 보안 모델링(Scenario based modeling)은 오래전부터 모델링 기법으로 사용되어 왔고, SCADA시스템의 사이버 보안 모델링 관련된 연구 논문 수도 가장 많은 편이다. 공격 그래프(Attack Graph)와 공격 트리(Attack Tree)는 3장에서 설명하며, 취약점

트리(Vulnerability Tree) 및 침해 트리(Compromise Tree)는 공격 트리와 유사한 기법이다. 다만 최종 노드의 상태가 취약점과 침해 상태를 나타낸다. 페트리넷(Petrinet)은 시스템 모델링 기법으로 많이 사용되며, 상태와 전이로 구성되어 있다. 침입탐지시스템 등의 설계에 많이 사용되어 왔다. CORAS는 위험분석을 하는 상용 모델링 기법중의 하나이다. 시나리오 기반 사이버 보안 모델링은 크게 아래와 같이 8단계 활동으로 구성되어 진다.

(1) 자산 식별 및 판별 (2) 발생 가능한 사이버 위협 발견 (3) 시간 순으로 발생 가능한 공격 시나리오 기술 (4) 존재하는 위험 분석 및 기존 사이버 침해 사례 분석 (5) 위협과 취약점 분석 (6) 시나리오별 공격 경로 식별 (7) 사이버 침해 영향의 확률적이고 정량적 크기 산출 (8) 결과 문서화 및 검토 이다[27]. 시나리오 기반 사이버 보안 평가기법은 적용 된지는 가장 오래되었지만, 평가자에 의해 주관적인 평가가 가능하고 정량화된 평가기법이 아닌 단점이 있어 핵심기반시설의 보안성 평가기법으로는 부적절한 점이 있다.

2.2 미국 전력연구원

미국 전력 분야 산업계의 연구원 EPRI(Electric Power Research Institute)는 전력 및 발전제어시스템 분야에 관한 사이버 보안 평가 및 조치 방법론인 TAM(Technical Assessment Methodology)을 발간하였다. TAM은 Fig. 2와 같이 총 5단계로 구성되어 있다[30]. EPRI TAM방법론의 가장 큰 특징은 공격 표면(attack surface)분석이다.

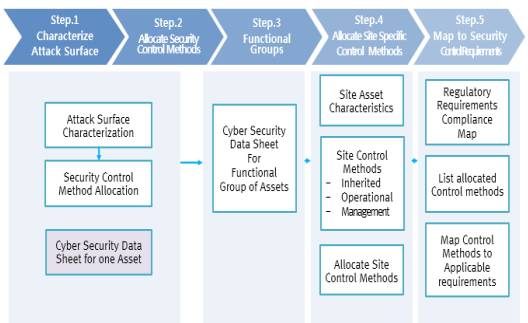

Fig. 2. EPRI TAM Process

공격 표면 분석은, 자산별로 사이버 보안 데이터 쉬트(CSDS)를 작성하여 자산의 취약점과 악용 가능한 공격 경로를 식별한다. 공격 표면 분석에서는 기술적 취약점을 다음과 같이 4개로 구분한 후 각 자산에 대해 악용 가능한 경로를 식별한다.

1. 즉각적 자산 기능 불능 초래
2. 지연적 자산 기능 불능 초래
3. 서비스 거부 초래
4. 악성 웨어 감염 초래

자산별로 작성하는 사이버 보안 데이터 쉬트는 총 56가지의 속성 정보의 기입이 필요하다. 자산별로 데이터 쉬트를 완성한 후, 자산에 존재하는 취약점과 악용 가능한 공격 경로를 파악한다. 기술적 취약점의 악용은 특정한 공격 경로에 의해서만 발생되기 때문에 감염 매커니즘 및 전파 경로를 찾는 것이 이 방법론의 가장 중요한 활동이다.

다만 사이버 보안 데이터 쉬트 작성시, 세부 펌웨어 및 어플리케이션 정보, 물리논리적 서비스 포트 정보단계까지 정보 획득이 필요하나, 자산 제조사가 제공하는 정보 이외에는 파악하기 어려운 점이 존재한다.

2.3 미국 원자력협회

최근 핵심기반시설 중에서 사이버 보안이 가장 중요시되고 주목받는 분야는 원자력발전소이다. 미국 등에서는 원자력 발전 사이버 보안 관련하여 다양한 보안 평가 기법 및 방법론을 제정하고 있다. 미국 원자력사업자 협회(Nuclear Energy Instutute)에서는 "NEI 13-10.Cyber Security Control Assessment"라는 사이버 보안 평가 방법론을 만들어 적용 중이다. Fig. 3은 NEI 13-10 보안 평가 모델링의 단계이다[31].

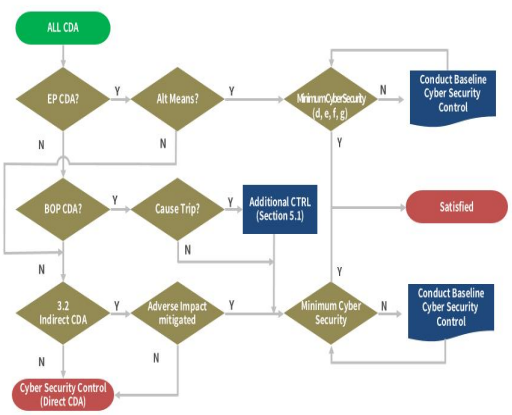

Fig. 3. NEI 13-10 Assessment Process

NEI 13-10 보안 평가 프로세스의 목적은 원자력 발전소 디지털 자산의 중요도 평가를 시행하는 것이다. 디지털 자산이 원전의 안전에 끼치는 영향을 측정하는 영향도 평가(Consequence Assessment)를 수행하여 총 8가지의 디지털 자산 유형으로 분류한 후, 중요도 등급의 차이에 따라 보안 조치 항목을 차등 적용하는 방법론이다. NEI 13-10 방법론은 미국에서 운영 중인 원자력 발전소에 대해 적용 가능하고 효율적 보안조치를 목적으로 하기 때문에, 사이버 보안 평가 및 이에 따른 보안 조치를 빠른 시간에 효율적으로 적용할 수 있는 방법론이다. 이는 미국 대부분의 가동 원자력 발전소에서 사용하고 있으며, 규제기관인 미국 원자력 위원회의 승인을 받은 방법론이다. 다만 날로 시스템의 연결이 복잡해지고 네트워크 연결성이 추가되는 디지털 계측제어시스템에 대해 세부적인 공격 경로를 파악하고 사전에 차단하기에는 부족한 점이 많아, 최근 건설 중인 미국 원자력 발전소에서는 NEI 13-10 방법론에, 다섯 가지 공격 벡터(Attack Vector) 기반의 취약점 분석을 추가하여 적용하는 추세이다.

3. 연구 내용

3.1 연구 방법

본 연구에서는 2장에서 살펴본 핵심기반시설의 사이버 보안 평가 모델링 사례에서 사용하고 있는 모델링 기법을 분류하고 각각의 특징을 파악하여 최적의 모델링 기법 의 방향을 제안하고자 한다. 먼저 2장에서 살펴본 사이버 보안 평가 모델링 사례에 나타난 기법들을 정량적인 방법과 정성적인 방법으로 구별할 수 있으며 이를 나타내면 Fig. 4와 같다.

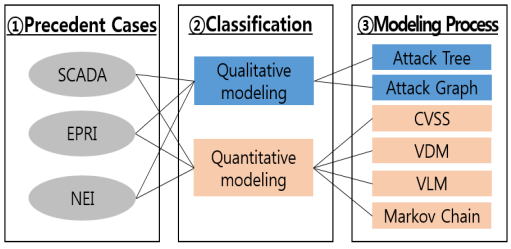

Fig. 4. Modeling Classification Process

3.2 정성적(Qualitative) 모델링 기법

3.2.1 공격 트리(Attack Tree)

공격 트리는 네트워크로 연결된 시스템에 대한 다양한 공격의 공격 경로를 파악하고, 이를 방어할 수 있는 보안 대책을 마련할 수 있도록 가시적이고 체계적인 방법을 제공한다. Fig. 5는 공격 트리의 구조를 보여준다.

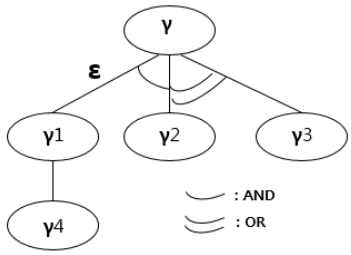

Fig. 5. Attack Tree

루트 노드는 공격의 최종 목적이나 대상을 나타내며, 최하위 노드와 중간 노드는 공격의 최종 목적을 이루기 위한 다양한 공격 방법을 나타낸다. 노드는 선택이 가능한 'OR' 노드와 목적을 달성하기 위해서는 필히 수행이 되어야 하는 'AND' 노드로 구성된다. 공격 트리는 세 가지 요소로 구성되는데, 엣지(ε), 정점(γ), 조합(θ)으로 이루어진다. 엣지(ε)는 자식 노드들에서 공격을 수행한 후, 부모 노드로 이동하는 공격 전이 상태의 집합을 의미하고, 정점(γ)은 공격 목표나 목적을 표현하는 노드들의 집합이다. 다만 공격 트리는 복잡하고 변형된 공격을 나타내는 데 한계가 있다. 공격 방법의 순서, 우선 순위, 악용 가능 수준 등의 정보를 나타내지 못하기 때문에 공격의 발생순서나 단계별 공격 진행에 따른 위험 수준을 판단할 수가 없다.

예를 들면, 반드시 노드들의 공격 이벤트가 순서대로 발생되어야 침입으로 판단될 수 있는 공격을, 공격 트리의 경우 공격 순서에 무관하게 공격 이벤트들이 공격 트리의 노드에 포함되기 때문에 침입이라고 판단하여 오탐을 발생할 수 있다.

3.2.2 공격 그래프(Attack Graph)

공격 그래프는 공격 트리의 단점을 보완하여 네트워크를 이루고 있는 시스템의 공격 경로 식별 및 보안 평가에서 유용한 도구로 사용되고 있다. 이는 가능한 모든 공격 경로를 파악하고, 악용 가능한 최적의 공격 경로를 식별할 수 있다. 공격 그래프는 공격 트리와 비슷한 모양을 가지고 있다. 공격 그래프에서 루트는 공격자를 나타낸

다. 간선은 목표 시스템에 접근하기 위해 공격자가 악용하는 취약점의 수를 의미한다. 공격자는 취약점이 있는 시스템에 연결된 또 다른 시스템들의 취약점을 악용해서 최종 목표까지 접근할 수 있다. 공격 그래프를 이용하면 실제 공격이 발생하는 모든 경로를 파악 할 수 있지만 한계점도 존재한다. 공격 그래프는 시간, 환경, 발생 가능성 등의 변수를 고려하지 못하며, 공격방법의 우선순위, 악용 수준 등의 다양한 정보를 반영하지 못한다. 앞에서 살펴본 스턱스넷(Stuxnet)같은 핵심 기반 시설에 대한 지능화되고 고도화된 사이버 공격을 분석하는데 한계가 존재한다.

3.3 정량적(Quantitative) 모델링 기법

3.3.1 공통 취약점 평가 체계(CVSS)

공통 취약점 관리체계, CVSS(Common Vulnerability Scoring System)는 상용 운영체제 및 어플리케이션의 취약점을 분석한 후 위험도를 수치화하여 점수로 계산하는 방식이다[32]. 2004년에 미국에서 2.0 버전으로 적용되어 2011년 4월에 국제 표준으로 공식 채택되었다. CVSS는 크게 기본 지수(Base Metrics), 임시 지수(Temporal Metrics), 환경 지수(Environmental Metrics)로 구분되며, 취약점 점수에 가장 큰 영향을 미치는 기본 지수의 경우 공격벡터, 접근 복잡도, 기밀성, 가용성, 무결성, 인증의 세부 항목으로 나뉘어져 있다[33]. 하지만 2.0 버전의 경우 인증, 접근 복잡도 등의 항목에서 세분화된 평가를 수행하기에 한계점이 존재하였으며. 이를 수정한 CVSS 3.0 버전이 2014년 공식 채택되었다. Fig. 6은 CVSS 3.0의 구조를 보여주고 있다.

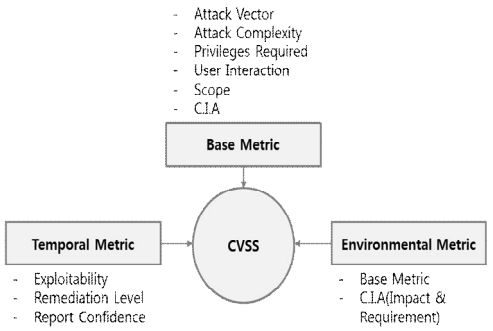

Fig. 6. CVSS 3.0 Structure

3.3.2 취약점 발견 모델(Vulnerability Detection Model)

취약점 발견모델은 시스템의 보안 취약점 발견에 대해 정량적으로 예측하는데 필요한 중요한 방법이다. 취약점 발견모델을 통해 취약점의 발견율 및 발견될 취약점의 누적 개수를 예측할 수 있다. 1998년, Alhazmi and Malaiya는 주요 OS를 대상으로 연구한 취약점 탐색 모델을 적용하였다. 그리고 연구한 모델과 실제 취약점 발견 수치와의 차이를 분석하기 위해 카이스퀘어 적합도 검정을 실시하였다. 시험 결과에 의하면 Alhazmi and Malaiya모델이 가장 많은 운영체제에서 발견된 취약점에서 유의함을 보였으며 이를 AML모델이라 한다[34]. AML은 시간의 경과를 기반으로 수행하는 취약점 발견 모델 중의 하나로서 S곡선 형태를 나타내는 로지스틱 모델이다. 이 모델은 취약점의 발견이 세 단계로 나누어 발생한다고 가정한다. 첫 번째 단계는 적응 단계이며, 새로운 소프트웨어가 시장에 배포되고 점차 사용되는 시기이다. 아직 소프트웨어 약점에 대한 파악이 완전히 이루어지지 않은 시점이기 때문에 취약점의 발견율이 낮은 상태이다. 두 번째 단계는 상승단계이며, 취약점 발견율이 급속도로 상승하게 되는 시점이다. 발견된 취약점에 대한 정보 공유가 활성화되고 취약점에 대한 공격이 급속도로 증가하는 시기이다. 마지막 단계는 포화 단계이다. 시스템의 발견하기 쉬운 취약점은 거의 발견이 된 상태이며, 시스템이 가지고 있는 한계 취약점의 개수에 도달하면서 취약점 발견율이 급속도로 낮아지게 된다.

3.3.3 취약점 생명 모델(Vulnerability Lifecycle Model)

취약점은 발견부터 전파 및 소멸까지 생명주기를 가지고 있다. 취약점은 발견 초기, 즉 패치 등이 공개되기 전에는 악용으로 인한 피해 크기 등이 지대하지만, 시간이 지나 취약점 패치등이 이루어지면 취약점 피해 크기도 줄어들게 된다. 이러한 취약점의 특징을 이용한 생애주기 관점에서의 모델링을 다루는 연구들을 살펴보면, 이런 연구들은 개별 취약점의 생명주기에 초점을 두고 있다. 하지만 실제 현장에서는 공격 목표를 침해하기 위해 여러 노드의 취약점들을 연계 및 악용하여 공격을 시도한다. 스턱스넷 같은 지능화된 사이버 위협 역시 여러 개의 취약점들을 연계한 취약점 체인을 이용하며 이를 킬체인(Kill Chain)이라고도 부른다. 그래서 여러 개의 취약점들이 서로 상호 연계되어 취약점 생애 주기 동안 어떠한 영향을 주는 지 분석이 필요하다.

4. 분석 결과 및 논의

4.1 정성적 모델링 기법의 특징 및 한계점

정성적 사이버 보안 위험 모델링의 목적은 핵심기반시설에 대해 실제적이고 악용 가능성이 큰 위협 경로를 파악하는 것이다. 이를 위해서 시간 및 상태 변화를 반영하여 동적으로 위협 경로를 판단하는 기법이 필요하다.

특히 핵심기반시설에 대한 위협 경로는 일반적인 IT 시스템과 다르게 위협 경로가 한정되어 있는 점을 고려할 필요가 있다. 이러한 핵심기반시설의 정성적 사이버 보안 위험 모델링이 가져야 할 특성을 아래 네 가지 요소로 나타낼 수 있다.

- **공격 순서 표현**: 여러 단계를 통해 수행되는 공격을 시간 순으로 구분하여 표현이 가능해야 한다.
- **침해 전제 조건 표현**: 해당 노드에 침해가 발생 가능한 전제 조건 및 상황을 표현해야 한다.
- **상태 변화 표현**: 시간에 따른 노드의 상태 변화 및 전이 가능 조건을 표현해야 한다.
- **동적 위협 경로 표현**: 시간 및 환경 변화에 따라 공격 전이 가능성을 동적으로 표현해야 한다.

앞서 살펴본 기존의 정성적 모델링 기법들이 위에서 정의한 특성을 지원하는지를 Table 2에 정리하였다.

Table 2. Classification of Qualitative modeling's characteristics

Characteristics	Scenario based	Attack Tree	Attack Graph
Attack Sequence expression	○	×	○
expression of Incident precondition	○	○	○
State Change expression	×	○	○
Dynamic threat path representation	×	×	△

기존 연구들 중에서, 이러한 특성을 모두 만족하는 기법은 동적 공격 그래프이다. 동적 공격 그래프는 공격 그래프의 한 종류이며, 시간이나 상태의 변화를 반영하고, 시스템이 취약한 상태를 정량적으로 표현해 줄 수 있다.

4.2 정량적 모델링 기법의 특징 및 한계점

정량적 사이버 보안 위험 모델링은, 객관적이고 정량적 수치를 이용하여 위험을 평가한다. 정량적 사이버 보안 위험 모델링 기법들이 나타내는 가장 큰 점은 정량적 지수 산출에 있어서 공신력과 객관성 있는 산출식이다. 이러한 핵심기반시설의 정량적 사이버 보안 위험 모델링 기법이 가져야 할 특성들을 아래 요소로 정리할 수 있다.

- **객관성**: 객관적인 산출식과 외부에 공신력 있는 산출 기법 제시 필요
- **시간 변화 반영**: 시간 경과에 따라 동적으로 정량적 보안지수 산출 필요
- **다양한 고려 요소**: 보안 모델링시 다양한 고려 요소를 포함한 정량적 보안 지수 산출 필요
- **범용성**: 정량적 산출 방식이 제어시스템등의 핵심기반시설에서 널리 사용

앞서 살펴본 기존의 정량적 모델링 기법들이 위에서 정의한 특성을 지원하는지를 Table 3에 정리하였다.

Table 3. Classification of Quantitative modeling's characteristics

Characteristics	CVSS	VDM	VLM
Objectivity	○	○	○
Reflection of TIme change	△	○	○
Various Considerations	○ (18)	× (5)	× (3)
Universality	○	△	△

기존 정량적 사이버 보안 위험 모델링 기법들이 위 네 가지 특성을 지원하는지 살펴보면 아래와 같다.

첫째, "객관성"에 대해서는 기존 세 가지 연구 모델링기법들이 모두 객관적인 산출방식 및 방법을 가지고 있다.

둘째, 시간 변화 반영 항목에서는 취약점 발견모델(VDM)과 취약점 생명모델(VLM)은 시간의 경과에 따른 정량적 지수 산출식을 제공한다. 공통 취약점 관리 체계(CVSS)의 경우 임시 지수(Temporal Metric)에서는 시간의 경과에 대한 산출 방식을 제공하나,영향 요소들이 세분화되어 있지 않고, 시간의 단위 역시 세분화 되어 있지 않다.

셋째, "다양한 고려요소"부분은 공통취약점 관리체계가 18개의 세부 고려 요소를 이용하여 산출되며, 취약점 생명주기 모델은 5개, 취약점 발견 모델의 경우 3개의 세부 구성요소로 산출이 되는데, 이는 누적 데이터를 기반으로 하는 특성 때문이다.

넷째, "범용성"에서는 공통취약점 관리체계 방식이 기존 IT시스템 분야 및 핵심기반시설의 일부분에서 널리

사용되고 있다. 취약점 발견 모델과 취약점 생명주기 모델의 경우 시장 점유율이 큰 일부 소프트웨어 중심으로 실제 사용되고 있지만, 핵심기반 시설 등에서 전반적으로 사용하지 않고 있다. 이유는 이 모델들의 경우 누적 데이터를 기반으로 사이버 보안 위험 모델링을 수행하며 핵심기반시설이 해당하는 제어시스템 분야에서는 이런 통계학적 누적 데이터가 많지 않기 때문이다.

5. 결론

기존 핵심기반시설을 구성하는 제어시스템은 특화된 운영체제 등이 사용되었지만, 최근에는 Windows등의 상용화된 범용 운영체제 사용이 증가하고 있다. 메인 서버 사용에서 X86급 워크스테이션, PC, 이동·무선매체 사용이 증가하고 있으며 Modbus, Fieldbuse등의 전용 프로토콜에서 TCP/IP등의 범용 프로토콜을 사용하고 있다.

이처럼 기존 핵심기반시설의 계측제어시스템이 디지털화됨에 따라, 계측제어시스템에 대한 사이버 침해가능성도 증가하고 있다.

이렇게 점차 디지털화되어가고 있는 핵심기반시설의 사이버 보안 위험을 정확하게 평가하고 예측하기 위해 기존의 연구들을 분석한 결과, 핵심기반시설의 사이버 보안평가 모델링의 요구사항을 Fig. 7 과 같이 도출하였다.

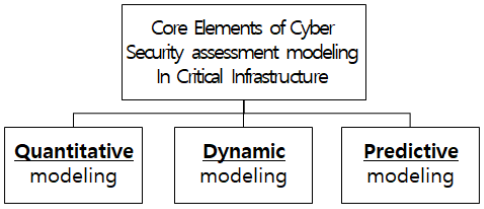

Fig. 7. Core Elements of modeling in Critical Infrastructure

첫 번째 핵심 요소는 정량적(Quantitative)모델링이다. 이는 정량적인 보안 모델링 수치를 적용하는 것으로 기존에 범용적으로 사용하고 있는 공통취약점평가체계(CVSS)의 스코어링 체계에 대해 핵심기반시설의 특징을 반영한 수정이 필요하다.

두 번째 핵심 요소는 동적(Dynamic)모델링이다. 이는 취약점이 시간 및 환경의 변화에 따른 영향의 크기를 반영하는 것으로 공격 그래프상에서 노드간의 전이확률 등에 대한 보완이 필요하다.

세 번째 핵심 요소는 예측 가능적(Predictive)모델링이다. 이는 알려져 있는 취약점들의 시간의 경과에 따른 보안 위협을 반영하는 것으로 취약점 생명주기 모델의 응용이 필요하다.

정량화된 보안지수의 기본은 기존 공통취약점 평가체계를 사용하며, 공통취약점 평가체계를 구성하는 핵심 요소를 응용하여 세부 구성 요소인 공격 벡터, 공격 복잡도, 인증 여부, 침해시 영향 크기(기밀성, 무결성, 가용성)등을 이용하는 것이다. 최근 기반시설의 제어시스템이 상용 운영체제가 탑재된 디지털 계측제어시스템이 많이 적용되고 있고 사이버 보안 활동의 중심이 되고 있다. 상용 운영체제의 취약점에 대한 핵심 지표중의 하나인 공통취약점평가체계(CVSS)를 중심으로, CVSS점수를 공격 그래프상 노드에 확률론적으로 적용한 확률기반 공격 그래프(Attack Graph based Probability)를 중심으로 한 모델링이 필요하다. 마지막으로, 예측 가능한 사이버 보안 평가를 위해, 취약점 발견 모델과 취약점 생명주기 모델을 시간 축을 중심으로 확률 기반 공격 그래프에 동시에 적용하여 시간의 경과에 따른 공격그래프 노드 간의 전이 확률을 동적으로 계산하는 연구 및 이를 실제 핵심기반시설의 테스트베드에 적용한 후 검증을 하는 것도 추후 연구가 필요하다.

REFERENCES

[1] *An Overview of Threat and Risk asseessment.* (2002). Newyork : SANS.

[2] R. Radvanovsky. & J. Brodsky.(2013). *Handbook of SCADA/Control Systems Security.* : CRC Press.

[3] E. Byres. & D. Leversage.(2007). Security incidents and trends in SCADA and process industries. *The industrial ethernet book, 39,* 26. DOI:10.1016/b978-0-12-397189-0.00002-1

[4] T. Gopal. M. Subbaraju. & R. Joshi. (2014). Methodology to articulate the requirements for security In SCADA. *fourth international conference on innovative computing technology,* 58-60. DOI:10.1109/INTECH.2014.6927744

[5] A. Cardenas. & S. Amin. (2011). Attacks against process control systems: risk assessment, detection, and response. *Proceedings of the 6th ACM symposium on information, computer and communications security,*. 121-123. DOI:10.1145/1966913.1966959

[6] J. Guan. & J. Hieb. (2011). A digraph model for risk identification and management in SCADA systems.

2011 IEEE international conference on intelligence and security informatics, 53-54.
DOI:10.1109/ISI.2011.5983990

[7] L. Durante. & A. Venzano. (2013). Review of security issues in industrial networks. *IEEE Trans Industry Information*, 35-36.
DOI:10.1109/tii.2012.2198666

[8] Y. Y. Haimes. & C. G. Chittester. (2005). A roadmap for quantifying the efficacy of risk management of information security and interdependent SCADA systems. *2005 IEEE international conference on intelligence and security informatics*, 72-74.
DOI:10.2202/1547-7355.1117

[9] G. Dondossola. & F. Garrone. (2009). Supporting cyber risk assessment of power control systems with experimental data. *Power systems conference and exposition, 2*, 36-38.
DOI:10.1109/PSCE.2009.4840170

[10] F. Baiardi. (2009). Hierarchical, model-based risk management of critical infrastructures. *Reliabilty Engineering System Safety journal, 94(9),* 1403-1415.
DOI:10.1016/j.ress.2009.02.001

[11] M. Warren. (2009). Safeguarding Australia from cyber-terrorism:a proposed cyber-terrorism SCADA risk framework for industry adoption. *Australian information warfare and security conference*, 23-27.
DOI:10.4225/75/57a7f3c09f482

[12] M. Franz. & D. Miller. (2004). The use of attack trees in assessing vulnerabilities in SCADA systems. *Proceedings of the international infrastructure survivability workshop, 1*, 42-44.

[13] G. Dondossola. & F. Garrone. (2009). Supporting cyber risk assessment of power control systems with experimental data. *Power systems conference and exposition, 3*, 12-15.
DOI:10.1109/PSCE.2009.4840170

[14] J. Szanto. (2011). Cyber risk assessment of power control systems metrics weighed by attack experiments. *Power and energy society general journal.* 112-116.
DOI:10.1109/PES.2011.6039589

[15] *Window of exposure a real problem for SCADA systems Recommendations for Europe on SCADA patching.*(2013).: ENISA

[16] G. N. Ericsson. (2009). Information security for electric power utilities (EPUs)-CIGR developments on frameworks, risk assessment, and technology. *IEEE Trans Power Delivery journal, 24(3)*, 1174-1181.
DOI: 10.1109/tpwrd.2008.2008470

[17] S. Grses. & M. Heisel. (2010). A comparison of security requirements SCADA engineering methods. *Requirements of Security Enginering journal, 15(1)*, 7-40.
DOI:10.1007/s00766-009-0092-x

[18] D. Thornton. & J. Dawson. (2012). Security best practices and risk assessment of SCADA and industrial control systems. *Proceedings of the 2012 world congress in computer science, computer engineering, and applied computing*, 111-114.
DOI:10.1109/rusautocon.2018.8501811

[19] R. Folkers. & J. Roberts. (2006). Scenario-based approach to risk analysis in support of cyber security. *Proceedings of the 5th international topical meeting on nuclear plant instrumentation controls, and human machine interface technology, 5(3)*, 293-300.
DOI:10.1002/sec.321

[20] R. Filippini. & M. Schimmer. (2012). Risk assessment methodologies for critical infrastructure protection. *European Commission Joint Research Centre Institute for the Protection and Security of the Citizen journal, 18*, 50-57.
DOI:10.1016/j.ijcip.2017.07.001

[21] K. Z. Snow. & D. R. Zaret. (2009). Evaluating the risk of cyber attacks on SCADA systems via Petri net analysis with application to hazardous liquid loading operations. *IEEE conference on technologies for homeland security*, 154-157.
DOI:10.1109/ths.2009.5168093

[22] S. Rudrapattana. & P. Kijsanayothin. (2014). Cyber security analysis of smart grid SCADA systems with game models. *Proceedings of the 9th annual cyber and information security research conference*, 143-145.
DOI:10.1145/2602087.2602089

[23] F. Massacci. & F. Paci. (2013). An experimental comparison of two risk-based security methods. *ACM/IEEE international symposium on empirical software engineering and measurement*, 182-186.
DOI:10.1109/ESEM.2013.29

[24] M. R. Permann. & K. Rohde. (2005). Cyber assessment methods for SCADA security. *15th annual joint ISA POWID/EPRI controls and instrumentation conference.*, .63-68.

[25] A. Zielstra. (2013). Assessing and improving SCADA security in the dutch drinking water sector. *Critical information infrastructure security journal,4(9),*124-134.
DOI:10.1016/j.ijcip.2011.08.002

[26] A. Krings. & J. Alves. (2012). Risk analysis and probabilistic survivability assessment an assessment approach for power substation hardening. *Proceedings of ACM workshop on scientific aspects of cyber terrorism.*
DOI:10.1109/isgt.2017.8085978

[27] D. Gertman. & R. Folker. (2006). Scenario based approach to risk analysis in support of cyber security. *Proceedings of the 5th international topical meeting on nuclear plant instrumentation controls, and human machine interface technology, 5(9),*293-300.
DOI:10.1002/sec.321

[28] S. Patel. & J. Graham. (2008). Quantitatively assessing the vulnerability of critical information systems. *new*

method for evaluating security enhancements International Journal, 28(9), 483-491.
DOI:10.1016/j.ijinfomgt.2008.01.009

[29] M. H. Henry. & R. M. Layer. (2009). Evaluating the risk of cyber attacks on SCADA systems via Petri net analysis with application to hazardous liquid loading operations. *IEEE conference on technologies for homeland security*. 76-79.
DOI:10.1109/ths.2009.5168093

[30] *Cyber Security Technical Assesment Methodology: Vulnerability Identification and Mitigation Overview of Threat and Risk asseessment.*(2016). Newyork : EPRI.

[31] *NEI 13-10 Cyber Security Control Assesment Rev5.*(2016). Washington D.C: Nuclear Energy Institute

[32] S. Y. Oh. & J. K. Hong. (2018). Vulnerability Case Analysis of Wireless Moving Vehicle. *journal of the Korea convergence society , 9(8),* 41-46.
DOI:10.15207/JKCS.2018.9.8.041

[33] J. K. Cho. (2019). Study on Improvement of Vulnerability Diagnosis Items for PC Security Enhancement. *Journal of Convergence for information Technology, 9(3),* 1-7.
DOI:10.22156/CS4SMB.2019.9.3.001

[34] O. H. Alhazmi. & Y. K. Malaiya. (2007).Measuring, Analyzing and Predicting Security Vulnerabilities in Software Systems. *Computers&Security journal, 26(3),* 219-228.
DOI:10.1016/j.cose.2006.10.002

엄 익 채(Ieck-Chae Euom) [정회원]

· 2003년 8월 : 전남대학교 컴퓨터정보학과(이학사)
· 2015년 2월 : 한국과학기술원 소프트웨어대학원(공학석사)
· 2019년 2월 : 전남대학교 정보보안협동과정(이학박사)
· 2007년 9월 ~ 현재 : 한전KDN(주) 보안컨설팅팀 재직중
· 관심분야 : 산업제어시스템 보안, 소프트웨어 개발 보안
· E-Mail : icelaken@gmail.com