Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.2, Apr. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.2.259

Attack Tree를 활용한 Game Theory 기반 보안 취약점 정량화 기법*

이 석 철,[1†] 이 상 하,[2] 손 태 식[1‡]
[1]아주대학교, [2]동서울대학교

Game Theory-Based Vulnerability Quantification Method Using Attack Tree*

Seokcheol Lee,[1†] Sang-Ha Lee,[2] Taeshik Shon[1‡]
[1]Ajou University, [2]Dong Seoul University

요 약

현대사회는 가정, 산업, 금융 등 다양한 분야에 IT 기술 기반 시스템이 도입되어 운영되고 있다. 사회의 안전을 보장하기 위해서는 사회 전반에 도입된 IT 시스템을 사이버 공격으로부터 보호해야하며, 이를 위해 시스템의 현재 보안 상태를 이해하고, 점검하는 것은 사이버 공격에 효과적으로 대응하기 위해 선결되어야 하는 과제이다. 본 논문에서는 보안 취약점을 점검하기 위해 사용되는 Game Theory 및 Attack Tree 방법론의 한계점을 분석하고, 두 방법론의 한계를 상호 보완한 보안 취약점 정량화 기법을 제안하여, 보다 객관적이고 체계적으로 보안 취약점을 점검할 수 있는 방법을 제공한다.

ABSTRACT

In modern society, IT technology based systems are introduced and operated in various fields such as home, industry, and finance. To ensure the safety of society, IT systems introduced throughout society should be protected from cyber attacks. Understanding and checking the current security status of the system is one of the important tasks to response effectively against cyber attacks. In this paper, we analyze limitations of Game Theory and Attack Tree methodologies used to inspect for security vulnerabilities. Based on this, we propose a security vulnerability quantification method that complements the limitations of both methodologies. This provides a more objective and systematic way to inspect for security weaknesses.

Keywords: Game Theory, Attack Tree, Vulnerability Quantification

I. 서 론

정보통신 기술이 발달함에 따라 Home IoT 기술이 도입된 Home Area Network부터 Industrial IoT 기술이 도입된 Industrial Control Network까지 다양한 시스템에 IT 기술들이 도입되고 있으며, 사이버 공격으로부터 이들을 보호하기 위해 사이버 보안 기술의 연구가 증가하고 있다.

사회 전반에 적용된 IT 시스템의 안보를 실현함에 있어 현재의 보안 현황을 이해하고, 점검하는 것은 향후 해당 시스템을 대상으로 수행되는 사이버 공격에 대응하는데 있어 매우 중요한 사항이다.

사이버 공격이 수행되는 과정과 그로 인한 영향을 분석하기 위해 Attack Tree, Attack Graph, Game Theory, CVSS(Common Vulnerability Scoring System) 등이 사용되고 있다[1-4]. 이 중 Attack Tree 또는 Game Theory를 사용하는 방법은 Tree 형태로 공격의 경로 및 영향을 표현하고

Received(02. 02. 2017), Modified(04. 04. 2017), Accepted(04. 05. 2017)
* 본 연구는 미래창조과학부 및 정보통신기술진행센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2017-2016-0-00304)
† 주저자, go467913@ajou.ac.kr
‡ 교신저자, tsshon@ajou.ac.kr(Corresponding author)

있다는 공통점을 갖고 있다. 하지만 Attack Tree의 경우 Root Node가 공격 대상 또는 목표를 나타내고 Leaf Node가 공격 행위를 표현하는 반면 Game Theory는 Root Node는 공격의 시점이며, Edge로 표현되는 행위의 결과 또는 영향을 Leaf Node에 표현한다는 차이점을 갖고 있다.

현재 사이버 보안 분야에 적용되고 있는 Attack Tree를 활용한 사이버 위협 분석 방법에서는 공격에 대한 대응 방안을 하나의 Node에 포함하여 다루는 등 명확히 표현하지 않기 때문에 보안 취약점에 대한 정확한 정량화가 어렵다는 한계가 있다. 반면, Game Theory는 Edge를 통해 공격 또는 대응과 관련된 행위를 표현하기 때문에 사이버 공격 및 대응 관련 행위에 대한 영향을 정량화하기에 용이하다. 그러나 Game Theory를 사이버 보안 분야에 적용하는 것에 대해 현재까지 진행된 연구는 각 행위에 대한 영향을 정량화하는 방법 및 기준을 모호하게 제시하고 있기 때문에 사회 주요 시스템의 보안 취약점을 정량화하는데 활용하기에는 객관성이 부족하다. 따라서 Game Theory를 보안 취약점 정량화 분야에 활용하기 위해서는 각 행위에 따른 영향을 객관적으로 산출하는 것이 필요하다. 실제로 Game Theory 연구 분야에서는 행위에 따른 영향을 객관적으로 수치화 하는 것을 가장 어렵고, 긴 시간이 요구되는 작업으로 인식하고 있다. 본 논문에서는 사이버 보안 분야에 Game Theory를 적용하는데 있어서의 신뢰성을 확보하기 위해 Attack Tree를 활용하여 공격 행위와 방어 행위에 대한 영향을 측정하는 방법을 제시한다. 제안된 방법을 통해 각 시스템의 보안 전문가는 보안 사고에 보다 효과적으로 대처할 수 있을 것으로 기대하며, 보다 안전한 시스템을 모델링하기 위한 참고 자료로 활용할 수 있다.

본 논문의 구성은 다음과 같다. 2장과 3장에서는 Attack Tree와 Game Theory의 개념 및 사이버 보안 분야와 관련된 연구를 통한 장단점을 분석한다. 4장에서는 본 논문에서 제안하는 Attack Tree를 활용한 Game Theory 기반 보안 정량화 기법에 대해 소개한다. 5장에서는 Attack Tree 및 Game Theory 각각을 단독으로 사용했을 경우와 제안하는 기법을 사용했을 경우를 비교, 분석한다. 마지막으로 6장에서는 본 논문의 결과와 향후 연구에 대해 언급한다.

II. 관련연구

경제학 분야를 주요 적용 대상으로 설계된 Game Theory는 [5]에서 활용된 것처럼 가정에 설치된 EMS(Energy Management System)의 발전-소비량을 통해 소비자 측면에서의 에너지소비에 대한 경제 정책을 연구하는 것뿐만 아니라 네트워크, 무선 통신 기술 등 IT 분야에 활용되고 있다[6]. 이러한 추세에서 사이버 환경에서 보안과 관련된 공격, 방어 행위의 효과를 분석하기 위해 Game Theory를 활용하는 연구가 진행되고 있다[7-10]. 특히 [10]에서는 스마트 그리드 SCADA(Supervisory Control and Data Acquisition) 시스템에 Game Theory를 적용하여 공격자와 보안 관리자의 행위에 대한 영향을 분석하였는데, 영향 정도를 산출하는데 사용된 변수 및 수치를 저자가 임의로 추정하여 설정하는 등 기존 연구에서는 행위에 대한 영향을 정량화하는데 필요한 객관적인 근거가 부족했다는 한계점이 있다.

사이버 공격 기술들 간의 연관성 및 순서를 표현할 수 있는 방법 중 하나인 Attack Tree는 [11]과 같이 일반 IT 네트워크 환경에서의 공격 시뮬레이션 시나리오를 도출하기 위해 활용되거나, [12]에서 연구한 것처럼 국가 기간시설의 사이버 보안 취약점을 정량화하기 위해 사용되는 등 사이버 보안 분야에서 빈번히 적용·연구되고 있다. 하지만 Attack Tree와 관련된 기존 연구에서는 공격자와 보안 관리자 간의 상호 작용(counteraction)을 고려하지 않아, 최근 [13],[14] 등과 같이 Attack—Defense Tree를 구축하여 사이버 공격과 그에 대한 대응 방안 간의 상관관계를 표현하기 위한 연구가 진행되고 있다.

III. 연구배경

3.1 게임 이론

게임이론(game theory)은 원래 경제학 분야를 주요 적용 대상으로 설계되었으나 정치, 통신기술, 전력계통 운영, 그리고 사이버 보안 등 다양한 분야에 활용되고 있다. Game이란 두 그룹 간의 전략적 상호 작용을 기술하고, 한 그룹의 전략적 선택의 결과에 따른 이익, 손실이 다른 그룹에 미치는 영향을 분석하는 것으로 다음 Table 1과 같이 경쟁 여부, 진행 방식, 정보, 표현 방식 등 네 가지 기준에 따라 분류할 수 있다[3].

Table 1. Categorization of Games

Whether Cooperative	Cooperative
	Competitive
Move Proceeding	Sequential
	Simultaneous
Given Information	Perfect
	Incomplete
Represented Form	Strategic
	Extensive

Game Theory를 활용함에 있어 가장 중요한 두 가지는 Game의 Player와 Player의 행위에 따른 성과(payoff)에 대한 값을 설정하는 것이다. 사이버 보안 분야에서는 Player를 공격자와 보안 관리자로 비교적 쉽게 설정할 수 있다. 하지만 공격 및 보안 행위에 대한 영향 값을 설정하는 것은 시스템 구조, 네트워크 설정, 보안제품 사용여부 등 다양한 변수가 존재하기 때문에 객관적인 수치를 도출하는데 다소 어려움이 따른다. 그러나 Game Model의 신뢰성을 갖추고 그로 인해 도출된 결과를 신용할 수 있도록 만들기 위해서는 객관적이고 합리적인 기준을 활용하여 Player의 행위에 따른 영향 값을 계산하는 것이 필수적이다.

3.2 공격 트리

공격 트리(attack tree)는 사이버 공격 기술들 간의 연관성 및 순서를 표현할 수 있는 방법 중 하나로 국가 기간시설의 사이버 보안 취약점 정량화에 활용되는 등 사이버 보안 분야에서 활용되고 있다.

Attack Tree는 Fig. 1과 같이 사이버 공격의 대상 또는 목표가 되는 것을 Root Node로 설정한 뒤, 목표를 달성하기 위해 선행되어야 하는 세부 공격 또는 작업을 Leaf Node(Sub Node)로 트리를 구성하는 Multi-layer 구조를 갖는다[1]. 트리는 구성하는 방법은 공격 대상을 설정한 뒤, 목적을 달성하기 위한 공격 수단을 찾고, 이를 트리로 구성하는 것이다. 이 때 구성한 트리는 다른 목적을 달성하기 위한 공격의 서브트리로 활용될 수 있다. 이는 Attack Tree의 가장 큰 장점으로 General Model을 구성하여 Sub-tree의 내용을 다른 Attack에 재사용할 수 있다는 것이다. 그러나 공격 행위의 시작노드가 어디서부터 인지 불분명하여 해당 공격의 위험도를 정확히 측정하기 힘들고, 공격에 대한 방어 행위가 각 Node에 포함되어 있어 각

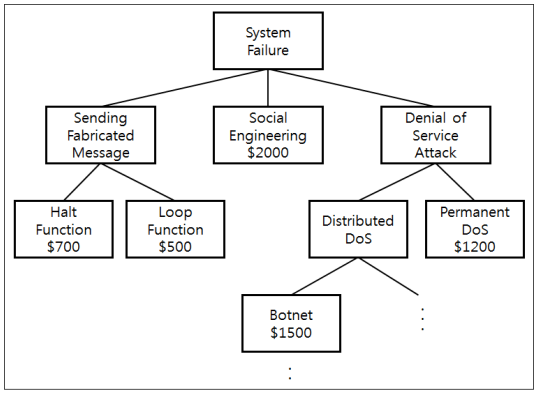

Fig. 1. Example of Simple Attack Tree

Node 별 세부 사항을 알 수 없어 사이버 공격에 필요한 공격 및 효과를 측정하는데 어려움이 있다.

3.3 상호 보완 방법

Game Theory를 활용하면, IT 시스템을 대상으로 하는 사이버 공격과 방어 행위 간의 상호 작용을 통한 사이버 공격 시나리오를 모델링 할 수 있다. 그러나 각 Player의 행위가 시스템에 미치는 영향을 객관적으로 수치화 할 수 있는 근거가 제시되어야 실제 시스템에 적용할 수 있다는 한계가 있다. 이를 보완하기 위해 본 논문에서는 사이버 공격과 방어 행위 단위 별 정량화에 적합한 Attack Tree를 활용하여 행위에 대한 비용 및 효과를 산출할 것이다. 제안하는 방법을 활용함으로써 Game Theory의 각 Player의 행위에 대한 효과를 산출하는데 있어 보다 명확한 근거를 제시할 수 있다.

IV. 공격 트리를 활용한 게임 이론 기반 보안 취약점 정량화 기법

본 장에서는 앞서 2장과 3장에서 분석한 Attack Tree와 Game Theory의 한계점을 보완하기 위해 Attack Tree를 활용하여 Game 에서의 Player의 행위에 따른 영향을 수치화하는 기법을 제안한다.

4.1 가정

본 논문에서 제안하는 Game Theory에서 Player는 공격자와 보안 관리자 두 명으로 설정하였으며, Game 유형은 두 Player가 경쟁하는 형태인

Non-cooperative(Competitive)방식, 그리고 한 Player가 행동을 취하면 다른 플레이어에게 순서가 돌아가는 Sequential Game이다. 그리고 Game 전략을 전개하기 위해서 각 Player가 취한 행위 내역들을 알고 있어야하기 때문에 각 Player의 행위는 상대방에게 알려지는 Perfect Information Game으로 가정한다.

4.2 제안 기법의 구성

제안된 기법은 다음 Fig. 2와 같이 크게 3가지 단계로 구성되어 있다. 첫 번째로 Game Theory 기반의 Attack-Defense Strategy Modelling을 수행한다. 두 번째로는 Attack Tree를 활용한 각 행위별 비용 및 영향을 분석해 수치화를 수행한다. 마지막으로, 각 State 별 공격자, 보안 관리자의 성과를 계산하여 대상 시스템의 보안 취약점을 정량화한다.

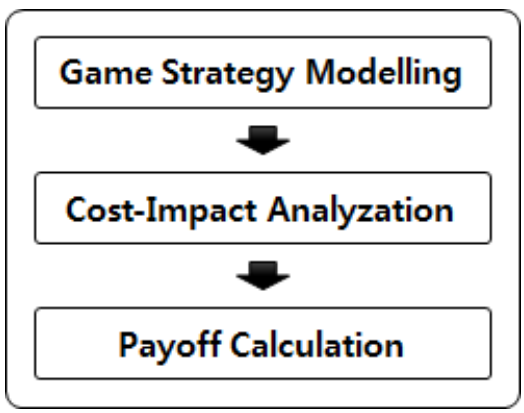

Fig. 2. Structure of Proposed Method

4.3 게임 전략 모델링

게임 전략 모델링(game strategy modelling) 단계에서는 정량화 대상 시스템에서 공격자와 보안 관리자 간의 행위(action)를 도출하고 각 행위 간 상호작용에 따른 상태(state) 변화를 도식화하는 트리 구조를 형성한다.

Game Strategy Model은 action과 state로 구성되는데 action은 공격자와 보안 관리자가 각각 취할 수 있는 공격 방법과 그에 대한 대응행위를 뜻한다. State는 공격자와 보안 관리자의 행위에 따른 상황을 나타내고 있으며, 해당 state까지 공격자와 보안 관리자의 action에 따른 성과정보를 포함한다.

Game Strategy Model을 구성하기 위해 크게 "공격-대응 action 도출"과 "반복적 state 생성" 두 가지 작업이 수행된다. 공격 action 도출은 Fig. 3과 같이 정량화 대상 시스템을 대상으로 설계된

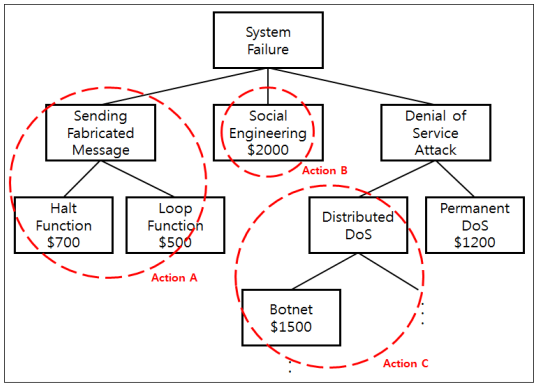

Fig. 3. Attack Action Deduction

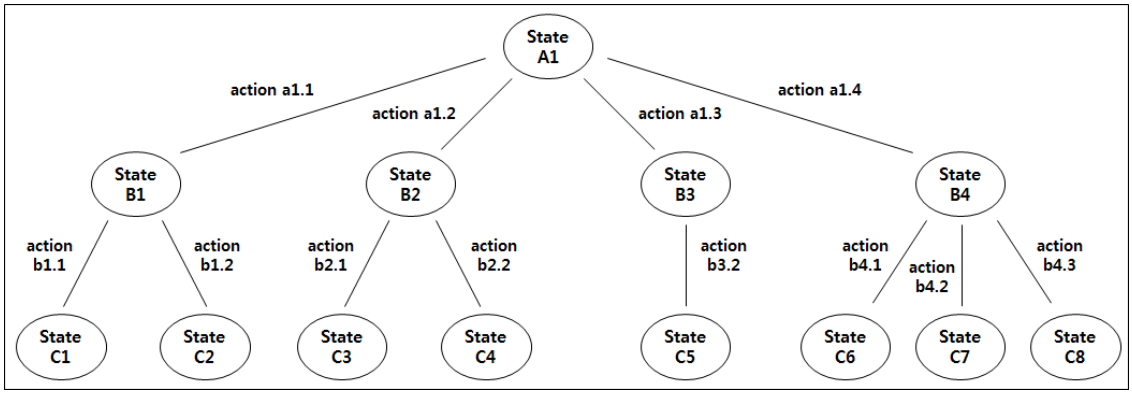

Fig. 4. Game Strategy Model Example

Attack Tree를 참조하여 유의미한 공격 action을 표현하는 Sub-Tree 그룹 단위로 공격 action을 식별한다. 대응 action의 경우에는 보안 장비 도입, 네트워크 설정 변경 등 보안 관리자가 공격자의 공격에 대응할 수 있는 방법들을 목록화하여 도출한다. 반복적 state 생성은 초기 상태에서 사용할 수 있는 공격 action을 root state에서 분배하여 차기 state를 생성한 뒤, 공격 action에서 생성된 state에서 해당 공격에 대한 대응 action들을 통해 branch를 생성하여 다음 state를 생성한다. 이와 같은 방법으로 공격-대응 action을 반복적으로 수행하며 state를 전개하며, Fig. 4와 같은 Game Strategy Model을 구축한다.

4.4 Cost-Impact 분석

Cost-Impact 분석 단계에서는 공격 및 대응 action의 cost를 산출한 뒤, 산출된 cost와 해당 공격의 위험도를 토대로 행위의 효과를 수치화한다. 그리고 정량화 대상 시스템의 특성에 따라 해당 action이 시스템에 미치는 영향을 계산한다.

1) 공격-대응 Action 별 cost 산출

Attack Tree를 참조하여 행위를 수행하는데 필요한 Cost를 계산한다. 공격자가 공격 a_i를 수행하는데 필요한 Cost는 행위 a_i를 구성하는 Attack Tree의 Sub Tree 내 비용의 총합으로 계산하며, 공격에 대응하여 보안 관리자가 취하는 행위의 Cost는 보안 장비 도입, 네트워크 설정 변경 등에 소요되는 비용으로 산정한다.

$$\mathrm{cost}(a_i) = \sum cost(sub\_actions\ of\ a_i) \qquad (1)$$

2) 공격-대응 Action에 따른 effect 분석

식 (1)으로부터 산출된 공격 action의 cost, 해당 공격의 성공 확률, 그리고 위험도를 통해 공격 action의 effect를 수치화하였다. 공격의 성공 확률은 0~1의 값을 갖는다. 위험도 $risk(a_i)$는 0~10의 값을 갖으며, 이 값은 CVE(Common Vulnerability & Exposures)를 참조하여 설정할 수 있다[15].

$$effect(a_i) = \mathrm{cost}(a_i) \times risk(a_i)^{p(a_i)} \qquad (2)$$

대응 action의 effect는 보안 관리자가 투자한 비용과 직전에 수행된 공격 action의 성공률 및 위험도를 통해 산출된다. 투자비용이 높을수록, 그리고 대응하는 공격이 성공률과 위험도가 높은 경우, 보안 측면에서 방어 action의 effect를 높게 평가할 수 있다.

$$effect(a_i) = \mathrm{cost}(a_i)^{p(a_{i-1})} \times risk(a_{i-1}) \qquad (3)$$

3) Action이 시스템에 미치는 Impact 분석

DoS(Denial of Service) 공격은 보안의 3요소 중, 가용성 측면에서 영향을 미친다. 이처럼 공격자의 공격 action이나, 이를 방어하기 위한 보안 관리자의 대응 action은 기밀성, 무결성, 가용성 각 측면에서의 영향이 모두 다르다[10]. 따라서 식 (4)와 같이 기밀성, 무결성, 가용성에 영향을 미치는지 여부에 따라 가중치를 부여한 뒤, 식 (2) 또는 식 (3)을 통해 산출된 action에 따른 effect 값에 곱해주는 방식으로 해당 action이 시스템에 미치는 영향을 계산한다. 이 때 가중치는 보안이 적용되는 대상 시스템의 특성에 따라 기밀성, 무결성, 가용성 각각의 중요도가 다르게 적용한다. 예를 들어, 일반 IT 환경에서는 가중치 〈w_c, w_i, w_a〉를 〈0.4, 0.3, 0.3〉로 설정하고, 가용성이 가장 중요한 보안 요소로 여겨지는 전력제어시스템 환경에서는 가중치를 〈0.2, 0.3, 0.5〉로 설정할 수 있다.

$$w(a_i) = w_c + w_i + w_a \ (0 < w(a_i) \leq 1) \qquad (4)$$

$$impact(a_i) = w(a_i) \times effect(a_i) \qquad (5)$$

4.5 Payoff 계산

식 (1)~(5)을 통해 계산된 cost, effect 분석을 통해 산출된 action이 시스템에 미치는 impact에 따른 Game Player의 payoff 변화는 Table 2와 같다. 공격자의 공격 action에 의해 공격자는 식 (6)만큼의 payoff를 얻으며, 이에 따라 보안 관리자는 식 (7)만큼의 payoff를 얻는다. 반면 보안 관리자의 대응 action에 의해서는 보안 관리자만 식 (8)만큼의 payoff를 얻고, 공격자의 payoff에는 영향을 미치지 않는다.

Table 2. Payoff Calculation for Each Player

	Adversary's Action	Security Admin's Action
Payoff of Adversary	$Impact(a_i) - \sum_{j=0}^{i} \lambda_j$ … (6)	-
Payoff of Security Administrator	$-Impact(a_i) + \sum_{j=0}^{i} \lambda_j$ … (7)	$Impact(a_i) + \lambda_j$ … (8)

식 (6)과 (7)에서 사용되고 있는 λ_i의 합계는 식 (9)와 같이 계산되는데, 이는 공격자와 보안 관리자의 action에 의한 payoff를 산정함에 있어 보안 관리자가 수행한 모든 대응 action에 의한 보정 값이다. 예를 들어 IDS(Intrusion Detection System)가 시스템에 도입되면 공격자의 공격이 쉽게 탐지되는 것처럼, 보안 관리자가 설치한 보안 장비 및 정책에 의해 시스템의 보안성이 향상되기 때문에 공격 action이 시스템에 미치는 영향이 감소된다.

$$\lambda_i = log(Impact(a_i)),\ (i = 2,4,6,...) \quad \cdots (9)$$

V. 토 론

본 장에서는 Game Theory 또는 Attack Tree 중 하나를 사용했을 경우와 본 논문에서 제안한 방법을 통해 시스템의 보안 취약성을 정량화하는 것을 다음 Table 3과 같이 비교 분석했다.

Game Theory만을 단독으로 사용하면 공격-대응 action에 대한 목록화를 수행하지 않기 때문에 state 별 상황에 따른 공격 경로 분석과 공격-대응 action에 대한 비용 산출이 어렵다. Attack Tree의 경우, 시스템 전체의 보안 취약성을 정량화하는 것 보다는 단일 단위의 공격을 분석하는데 적합하며, 공격자와 보안 관리자 간의 상호 대응 시나리오 작성에 어려움이 따른다.

본 논문에서 제안한 방법은 공격-대응 action에 대한 목록화를 수행함으로써 state 별 상황에 따른 공격 경로의 분석과 시스템 전반에 대해 공격자와 보안 관리자 간의 상호 대응 시나리오 작성이 가능하다. 또한 Attack Tree와 CVE를 통해 산출한 공격 action의 비용과 위험정도를 활용하여 보안 취약성을 정량화하기 위한 객관적인 근거로 활용할 수 있다.

Table 3. Comparison to other methods

	Game Theory	Attack Tree	Proposed Idea
Attack Path Analyzation	△	○	○
Attack Cost Consideration	-	○	○
Scenario Info Availability	○	-	○
Adversary-Sec_Admin Interaction	○	△	○

VI. 결론 및 향후 연구

본 논문에서는 시스템의 보안 취약점을 점검하기 위해 사용되는 Game Theory 및 Attack Tree 방법론의 한계점을 분석하였다. 기존 방법론의 경우 공격 및 대응 행위를 위해 투자된 비용 대비 효과를 정량화 하는데 객관성의 떨어지고, 공격자와 보안 관리자 간의 상호 대응행위의 시나리오를 도출하는데 어려움이 있었다. 이와 같은 한계를 보완하기 위해 본 논문에서는 'Game Strategy Modelling', 'Cost-Impact Analyzation', 그리고 'Payoff Calculation' 등 3단계로 구성된 Attack Tree를 활용한 Game Theory 기반 보안 취약점 정량화 기법을 제안하였다.

특히, 'Cost-Impact Analyzation' 단계는 기존 Game Theory에서 활용하고 있지 않은 Attack Tree, CVE 등 객관적인 근거에 기반 하여 공격자 및 보안 관리자의 행위가 시스템에 작용하는 영향을 수치화할 수 있다. 따라서 보안 관리자는 제안하는 기법을 통해 보안 취약점 정량화 대상 시스템의 보안 취약점을 객관적으로 산출할 수 있으며, 공격자의 공격 경로와 공격 행위에 대한 대응 방안을 사전에 예측 및 준비할 수 있을 것이다.

향후 연구에서는 본 논문에서 제안하고 기법을 Home IoT 기반 Home Area Network 및 Industrial IoT 기반 전력제어시스템에 적용한 사례 분석과 CVSS, MTTC 등의 취약성 정량화 기법과의 비교 분석을 수행할 예정이다.

References

[1] B. Schneier, "Attack Trees," Dr. Dobb's Journal, Oct. 1999.

[2] R. Lipmann and K. Ingols, "An annotated review of past papers on attack graphs," Tech. Rep., Lincoln Laboratory, Mar. 2005.

[3] Osborne, M. J. and Rubinstein, A, "A Course in Game Theory," The MIT Press, Jan. 2014.

[4] First.org, Inc., "Common Vulnerability Scoring System v3.0," Jun. 2015.

[5] R. Arai, K. Yamamoto, T. Nishio, and M. Morikura, "Differential game-theoretic framework for a demand-side energy management system," Proc. IEEE SmartGridComm 2013, Vancouver, Canada, Oct. 2013.

[6] M. Felegyhazi, J.-P. Hubaux, "Game Theory in Wireless Networks: A Tutorial", EPFL Technical Report LCA-REPORT-2006 - 002, Feb. 2006.

[7] W. He, et al, "A Game Theoretical Attack-Defense Model Oriented to Network Security Risk Assessment", International Conference on Computer Science and Software Engineering, Dec. 2008.

[8] Boehmer W, "Dynamic Systems Approach to Analyzing Event Risks and Behavioral Risk with Game Theory," IEEE Third international conference on Privacy, security, risk and trust and social computing, Oct. 2011.

[9] X. Liang and Y. Xiao, "Game Theory for Network Security," in IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 472-486, First Quarter 2013.

[10] R. Hewett, S. Rudrapattana and P. Kijsanayothin, "Smart Grid security: Deriving informed decisions from cyber attack game analysis," 2014 IEEE International Conference on Smart Grid Communications (Smart GridComm), Venice, Nov. 2014.

[11] Jung-kuk Seo et al, "Adapted Attack Tree for Internet Attack Simulation," Proceedings of Symposium of the Korean Institute of communications and Information Sciences, Nov. 2002.

[12] C. W. Ten, C. C. Liu and M. Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees," 2007 IEEE Power Engineering Society General Meeting, Tampa, FL, Feb. 2007.

[13] Du S. and Zhu H, "Attack-Defense Tree Based Security Assessment," Security Assessment in Vehicular Net works, Springer New York, Oct. 2013.

[14] X. Ji, H. Yu, G. Fan and W. Fu, "Attack-defense trees based cyber security analysis for CPSs," 2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Shanghai, May. 2016.

[15] Common Vulnerabilities and Exposures, "https://cve.mitre.org/"

〈저자소개〉

이 석 철 (Seokcheol Lee) 학생회원
2012년 2월: 아주대학교 정보 및 컴퓨터공학부 공학사
2012년 3월~현재: 아주대학교 컴퓨터공학과 석박사통합과정
〈관심분야〉 스마트그리드 보안, 디지털 포렌식, 네트워크 보안

이 상 하 (Sang-Ha Lee) 정회원
1987년 2월: 울산대학교 전자계산학과 졸업
1991년 2월: 아주대학교 컴퓨터공학과 석사
2002년 8월: 아주대학교 컴퓨터공학과 박사
1991년~1992년: (주)큐닉스 컴퓨터
1993년~1999년: (주)케이엔아이시스템
2000년~현재: 동서울대학교 정보통신과 근무
〈관심분야〉 디지털 포렌식, 네트워크 보안, IPTV QoS/ QoE, IoT

손 태 식 (Taeshik Shon) 종신회원
2000년: 아주대학교 정보및컴퓨터공학부 졸업(학사)
2002년: 아주대학교 정보통신전문대학원 졸업(석사)
2005년: 고려대학교 정보보호대학원 졸업(박사)
2004년~2005년: University of Minnesota 방문연구원
2005년~2011년: 삼성전자 통신/DMC 연구소 책임연구원
2011년~현재: 아주대학교 정보통신대학 사이버보안학과 부교수
2017년~현재: Illinois Institute of Technology 방문교수
〈관심분야〉 산업제어시스템 보안, 비정상행위탐지, 디지털 포렌식