(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년06월01일
(11) 등록번호 10-2117696
(24) 등록일자 2020년05월26일

(51) 국제특허분류(Int. Cl.)
G06F 21/57 (2013.01) *G06F 21/55* (2013.01)
H04L 29/06 (2006.01)
(52) CPC특허분류
G06F 21/577 (2013.01)
G06F 21/55 (2013.01)
(21) 출원번호 10-2018-0066362
(22) 출원일자 2018년06월08일
심사청구일자 2018년06월08일
(65) 공개번호 10-2019-0139642
(43) 공개일자 2019년12월18일
(56) 선행기술조사문헌
WO2008139856 A1*
JP2009110177 A*
KR1020060027748 A
JP2018032355 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
아주대학교산학협력단
경기도 수원시 영통구 월드컵로 206 (원천동)
(72) 발명자
손태식
경기도 수원시 영통구 월드컵로 206
이석철
경기도 부천시 심곡로22번길 22
(74) 대리인
심경식, 홍성욱

전체 청구항 수 : 총 7 항 심사관 : 구대성

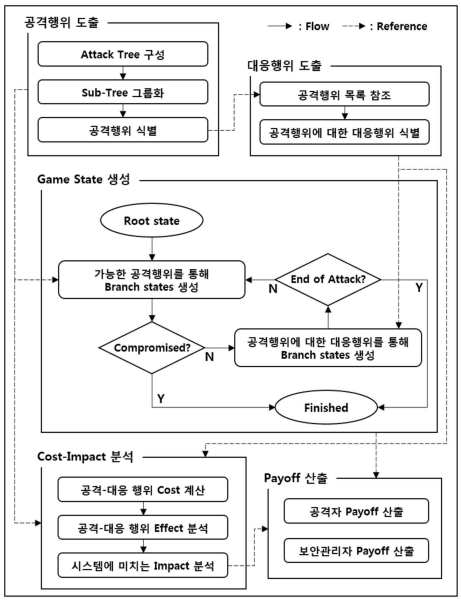
(54) 발명의 명칭 **게임 이론을 이용한 보안 취약점 정량화 방법 및 장치**

(57) 요 약

게임 이론을 이용한 보안 취약점 정량화 방법은, 보안 취약점 정량화 장치가, 공격자와 방어자가 참여하는 게임 이론(game theory)에 기초하여, 상기 공격자의 공격 행동과 상기 방어자의 방어 행동을 게임 전략 모델로 모델링하는 단계; 보안 취약점 정량화 장치가, 상기 게임 전략 모델의 각 상태 노드마다 해당 상태 노드에 이르게 된

(뒷면에 계속)

대 표 도 - 도2



상기 공격 행동 또는 상기 방어 행동을 수행하기 위해 비용(cost)을 계산하고, 상기 비용에 기초해서 상기 공격 행동 또는 상기 방어 행동으로 인한 효과(effect)를 계산하고, 상기 효과에 기초해서 상기 공격 행동 또는 상기 방어 행동이 미치는 영향(impact)을 계산하는 단계; 보안 취약점 정량화 장치가, 상기 영향에 기초해서 상기 게임 전략 모델의 각 상태 노드마다 상기 공격자의 보상(payoff)와 상기 방어자의 보상(payoff)를 계산하는 단계; 및 상기 방어자의 보상의 값과 각 상태 노드의 깊이에 따른 상기 방어자의 보상의 차이에 기초하여 보안 취약점을 방어할 우선 순위를 산출하는 단계를 포함할 수 있다.

(52) CPC특허분류
H04L 63/1433 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 2015R1A1A1A05001238
부처명 미래창조과학부
연구관리전문기관 한국연구재단
연구사업명 신진연구자지원사업(후속연구지원)
연구과제명 IoT 환경에서 APT공격 대응을 위한 전력기반시설 플랫폼 및 서비스 융합보안 기술
기 여 율 1/1
주관기관 아주대학교 산학협력단
연구기간 2017.05.01 ~ 2018.04.30
공지예외적용 : 있음

명 세 서

청구범위

청구항 1

보안 취약점 정량화 장치가, 공격자와 방어자가 참여하는 게임 이론(game theory)에 기초하여, 상기 공격자의 공격 행동과 상기 방어자의 방어 행동을 게임 전략 모델로 모델링 하는 단계;

상기 보안 취약점 정량화 장치가, 상기 게임 전략 모델의 각 상태 노드마다 해당 상태 노드에 이르게 된 상기 공격 행동 또는 상기 방어 행동을 수행하기 위한 비용(cost)을 계산하고, 상기 비용에 기초해서 상기 공격 행동 또는 상기 방어 행동으로 인한 효과(effect)를 계산하고, 상기 효과에 기초해서 상기 공격 행동 또는 상기 방어 행동이 미치는 영향(impact)을 계산하는 단계;

상기 보안 취약점 정량화 장치가, 상기 영향에 기초해서 상기 게임 전략 모델의 각 상태 노드마다 상기 공격자의 보상(payoff)와 상기 방어자의 보상(payoff)를 계산하는 단계; 및

상기 방어자의 보상의 값과 각 상태 노드의 깊이에 따른 상기 방어자의 보상의 차이에 기초하여 보안 취약점을 방어할 우선 순위를 산출하는 단계를 포함하고,

상기 게임 전략 모델로 모델링 하는 단계는,

상기 공격자의 제1 공격 행동으로 인한 제1 상태 노드를 생성하고, 상기 공격자의 제1 공격 행동에 대응하는 상기 방어자의 제1 방어 행동으로 인한 제2 상태 노드를 상기 제1 상태 노드의 자식 노드로 생성하는 단계를 포함하고,

상기 공격자의 보상(payoff)와 상기 방어자의 보상(payoff)를 계산하는 단계는,

상기 제1 상태 노드의 영향을 상기 제2 상태 노드의 공격자의 보상으로 계산하고, 상기 제1 상태 노드의 영향의 음의 값에 상기 제2 상태 노드의 영향을 더한 값을 상기 제2 상태 노드의 방어자의 보상으로 계산하는 단계; 및

상기 제1 상태 노드 또는 상기 제2 상태 노드의 상위 노드 중에 방어자의 방어 행동으로 인한 상태 노드의 영향의 값을 모두 더하고, 더한 값을 로그를 취하고, 로그를 취한 값을 이용하여 상기 공격자의 보상과 상기 방어자의 보상을 보정하는 단계

를 더 포함하는 것을 특징으로 하는 게임 이론을 이용한 보안 취약점 정량화 방법.

청구항 2

제1항에 있어서,

상기 게임 전략으로 모델링 하는 단계는,

상기 공격자의 공격 가능한 각각의 공격 경로를 공격 트리(attack tree)로 구성하는 단계를 포함하는,

게임 이론을 이용한 보안 취약점 정량화 방법.

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 영향(impact)을 계산하는 단계는,

상기 게임 전략 모델에 속한 제1 상태 노드의 하위 노드의 비용을 모두 합한 값을 상기 제1 상태 노드의 비용으로 계산하는 단계를 포함하는,

게임 이론을 이용한 보안 취약점 정량화 방법.

청구항 5

제1항에 있어서,

상기 영향(impact)을 계산하는 단계는,

상기 제1 공격 행동의 위험도에 상기 제1 공격 행동의 성공 확률을 지수승한 값을 상기 제1 상태 노드의 비용에 곱한 값을 상기 제1 상태 노드의 효과로 계산하는 단계를 포함하는,

게임 이론을 이용한 보안 취약점 정량화 방법.

청구항 6

제1항에 있어서,

상기 영향(impact)을 계산하는 단계는,

상기 제2 상태 노드의 비용에 상기 제1 공격 행동의 성공 확률을 지수승한 값을 상기 제1 공격 행동의 위험도에 곱한 값을 상기 제2 상태 노드의 효과로 계산하는 단계를 포함하는,

게임 이론을 이용한 보안 취약점 정량화 방법.

청구항 7

제1항에 있어서,

상기 영향(impact)을 계산하는 단계는,

분석 대상 시스템의 기밀성, 무결성, 가용성에 따른 각각의 가중치를 설정하는 단계;

상기 제1 공격 행동이 상기 분석 대상 시스템의 기밀성, 무결성, 가용성에 영향을 미치는지 여부에 따라 각각의 가중치를 합하여 상기 제1 공격 행동의 가중치를 계산하는 단계; 및

상기 제1 공격 행동의 가중치를 상기 제1 상태 노드의 효과에 곱한 값을 상기 제1 상태 노드의 영향으로 계산하고, 상기 제1 공격 행동의 가중치를 상기 제2 상태 노드의 효과에 곱한 값을 상기 제2 상태 노드의 영향으로 계산하는 단계를 포함하는,

게임 이론을 이용한 보안 취약점 정량화 방법.

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

공격자와 방어자가 참여하는 게임 이론(game theory)에 기초하여, 상기 공격자의 공격 행동과 상기 방어자의 방어 행동을 게임 전략 모델로 모델링 하는 게임 전략 모델링부;

상기 게임 전략 모델의 각 상태 노드마다 해당 상태 노드에 이르게 된 상기 공격 행동 또는 상기 방어 행동을 수행하기 위한 비용(cost)을 계산하고, 상기 비용에 기초해서 상기 공격 행동 또는 상기 방어 행동으로 인한 효과(effect)를 계산하고, 상기 효과에 기초해서 상기 공격 행동 또는 상기 방어 행동이 미치는 영향(impact)을 계산하는 비용-영향 분석부;

상기 영향에 기초해서 상기 게임 전략 모델의 각 상태 노드마다 상기 공격자의 보상(payoff)와 상기 방어자의 보상(payoff)를 계산하는 보상 계산부; 및

상기 방어자의 보상의 값과 각 상태 노드의 깊이에 따른 상기 방어자의 보상의 차이에 기초하여 보안 취약점을 방어할 우선 순위를 산출하는 우선 순위 산출부를 포함하고,

상기 게임 전략 모델링부는 상기 공격자의 제1 공격 행동으로 인한 제1 상태 노드를 생성하고, 상기 공격자의 제1 공격 행동에 대응하는 상기 방어자의 제1 방어 행동으로 인한 제2 상태 노드를 상기 제1 상태 노드의 자식 노드로 생성하고,

상기 보상 계산부는 상기 제1 상태 노드의 영향을 상기 제2 상태 노드의 공격자의 보상으로 계산하고, 상기 제1 상태 노드의 영향의 음의 값에 상기 제2 상태 노드의 영향을 더한 값을 상기 제2 상태 노드의 방어자의 보상으로 계산하고, 상기 제1 상태 노드 또는 상기 제2 상태 노드의 상위 노드 중에 방어자의 방어 행동으로 인한 상태 노드의 영향의 값을 모두 더하고, 더한 값을 로그를 취하고, 로그를 취한 값을 이용하여 상기 공격자의 보상과 상기 방어자의 보상을 보정하는 것을 특징으로 하는 게임 이론을 이용한 보안 취약점 정량화 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 게임 이론을 이용한 보안 취약점 정량화 방법 및 그 장치에 관한 것이다. 보다 자세하게는 게임 이론을 이용하여 시스템의 보안 취약점을 분석하고, 분석한 보안 취약점을 정량화 하는 방법 및 그 방법을 수행하는 장치에 관한 것이다.

배 경 기 술

[0002] 현대 사회에서 정보 통신 기술(ICT)은 가정, 산업 및 금융과 같은 다양한 분야에 적용되고 있다. 정보 통신 기술은 각각의 분야에 맞게 시스템을 구성하고, 해당 시스템에서 필요로 하는 어플리케이션을 개발 및 운영하고 있다. 이러한 애플리케이션의 안전성을 보장하려면 네트워크를 통한 공격으로부터 시스템의 보호가 필요하다.

[0003] 다양한 보안 기술 및 제품이 네트워크를 통한 공격으로부터 시스템을 보호하기 위한 목적으로 개발되었다. 네트워크를 통한 공격으로부터 시스템을 보호할 때 가장 중요한 것은 시스템의 현재 보안 상태를 파악하는 것이다. 즉, 실제 공격이 일어나기 전에 시스템의 취약점을 사전에 파악하고 이를 예방하는 것이 매우 중요하다.

[0004] 종래에도 네트워크 시스템의 보안 취약성을 검사하기 위한 다양한 유형의 취약성 정량화 방법이 개발되어 왔다. 그러나 기존의 방법은 정량화 결과에 객관성이 부족하다는 단점이 있다. 이에 객관성을 확보한 시스템 취약점 분석 방법에 대한 연구가 필요하다.

발명의 내용

해결하려는 과제

[0005] 본 발명이 해결하고자 하는 기술적 과제는 게임 이론을 이용한 보안 취약점 정량화 방법 및 장치를 제공하는 것이다.

[0006] 본 발명의 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0007] 본 발명의 일 실시예에 따른 게임 이론을 이용한 보안 취약점 정량화 방법은, 보안 취약점 정량화 장치가, 공격자와 방어자가 참여하는 게임 이론(game theory)에 기초하여, 상기 공격자의 공격 행동과 상기 방어자의 방어 행동을 게임 전략 모델로 모델링 하는 단계; 상기 보안 취약점 정량화 장치가, 상기 게임 전략 모델의 각 상태 노드마다 해당 상태 노드에 이르게 된 상기 공격 행동 또는 상기 방어 행동을 수행하기 위해 비용(cost)을 계산하고, 상기 비용에 기초해서 상기 공격 행동 또는 상기 방어 행동으로 인한 효과(effect)를 계산하고, 상기 효과에 기초해서 상기 공격 행동 또는 상기 방어 행동이 미치는 영향(impact)을 계산하는 단계; 상기 보안 취약점 정량화 장치가, 상기 영향에 기초해서 상기 게임 전략 모델의 각 상태 노드마다 상기 공격자의 보상(payoff)와 상기 방어자의 보상(payoff)를 계산하는 단계; 및 상기 방어자의 보상의 값과 각 상태 노드의 깊이에 따른 상기 방어자의 보상의 차이에 기초하여 보안 취약점을 방어할 우선 순위를 산출하는 단계를 포함할 수 있다.

[0008] 바람직하게는, 상기 게임 전략으로 모델링 하는 단계는, 상기 공격자의 공격 가능한 각각의 공격 경로를 공격

트리(attack tree)로 구성하는 단계를 포함할 수 있다.

[0009] 바람직하게는, 상기 게임 전략으로 모델링 하는 단계는, 상기 공격자의 제1 공격 행동으로 인한 제1 상태 노드를 생성하고, 상기 공격자의 제1 공격 행동에 대응하는 상기 방어자의 제1 방어 행동으로 인한 제2 상태 노드를 상기 제1 상태 노드의 자식 노드로 생성하는 단계를 포함할 수 있다.

[0010] 바람직하게는, 상기 영향(impact)을 계산하는 단계는, 상기 게임 전략 모델에 속한 제1 상태 노드의 하위 노드의 비용을 모두 합한 값을 상기 제1 상태 노드의 비용으로 계산하는 단계를 포함할 수 있다.

[0011] 바람직하게는, 상기 영향(impact)을 계산하는 단계는, 상기 제1 공격 행동의 위험도에 상기 제1 공격 행동의 성공 확률을 지수승한 값을 상기 제1 상태 노드의 비용에 곱한 값을 상기 제1 상태 노드의 효과로 계산하는 단계를 포함할 수 있다.

[0012] 바람직하게는, 상기 영향(impact)을 계산하는 단계는, 상기 제2 상태 노드의 비용에 상기 제1 공격 행동의 성공 확률을 지수승한 값을 상기 제1 공격 행동의 위험도에 곱한 값을 상기 제2 상태 노드의 효과로 계산하는 단계를 포함할 수 있다.

[0013] 바람직하게는, 상기 영향(impact)을 계산하는 단계는, 분석 대상 시스템의 기밀성, 무결성, 가용성에 따른 각각의 가중치를 설정하는 단계; 상기 제1 공격 행동이 상기 분석 대상 시스템의 기밀성, 무결성, 가용성에 영향을 미치는지 여부에 따라 각각의 가중치를 합하여 상기 제1 공격 행동의 가중치를 계산하는 단계; 및 상기 제1 공격 행동의 가중치를 상기 제1 상태 노드의 효과에 곱한 값을 상기 제1 상태 노드의 영향으로 계산하고, 상기 제1 공격 행동의 가중치를 상기 제2 상태 노드의 효과에 곱한 값을 상기 제2 상태 노드의 영향으로 계산하는 단계를 포함할 수 있다.

[0014] 바람직하게는, 상기 공격자의 보상(payoff)와 상기 방어자의 보상(payoff)를 계산하는 단계는, 상기 제1 상태 노드의 영향을 상기 제1 상태 노드의 공격자의 보상으로 계산하고, 상기 제1 상태 노드의 영향의 음의 값을 상기 제1 상태 노드의 방어자의 보상으로 계산하는 단계를 포함할 수 있다.

[0015] 바람직하게는, 상기 공격자의 보상(payoff)와 상기 방어자의 보상(payoff)를 계산하는 단계는, 상기 제1 상태 노드의 영향을 상기 제2 상태 노드의 공격자의 보상으로 계산하고, 상기 제1 상태 노드의 영향의 음의 값에 상기 제2 상태 노드의 영향을 더한 값을 상기 제2 상태 노드의 방어자의 보상으로 계산하는 단계를 더 포함할 수 있다.

[0016] 바람직하게는, 상기 공격자의 보상(payoff)와 상기 방어자의 보상(payoff)를 계산하는 단계는, 상기 제1 상태 노드 또는 상기 제2 상태 노드의 상위 노드 중에 방어자의 방어 행동으로 인한 상태 노드의 영향의 값을 모두 더하고, 더한 값을 로그를 취하고, 로그를 취한 값을 이용하여 상기 공격자의 보상과 상기 방어자의 보상을 보정하는 단계를 포함할 수 있다.

[0017] 본 발명의 다른 실시예에 따른 게임 이론을 이용한 보안 취약점 정량화 장치는, 공격자와 방어자가 참여하는 게임 이론(game theory)에 기초하여, 상기 공격자의 공격 행동과 상기 방어자의 방어 행동을 게임 전략 모델로 모델링 하는 게임 전략 모델링부; 상기 게임 전략 모델의 각 상태 노드마다 해당 상태 노드에 이르게 된 상기 공격 행동 또는 상기 방어 행동을 수행하기 위해 비용(cost)을 계산하고, 상기 비용에 기초해서 상기 공격 행동 또는 상기 방어 행동으로 인한 효과(effect)를 계산하고, 상기 효과에 기초해서 상기 공격 행동 또는 상기 방어 행동이 미치는 영향(impact)을 계산하는 비용-영향 분석부; 상기 영향에 기초해서 상기 게임 전략 모델의 각 상태 노드마다 상기 공격자의 보상(payoff)와 상기 방어자의 보상(payoff)를 계산하는 보상 계산부; 및 상기 방어자의 보상의 값과 각 상태 노드의 깊이에 따른 상기 방어자의 보상의 차이에 기초하여 보안 취약점을 방어할 우선 순위를 산출하는 우선 순위 산출부를 포함할 수 있다.

발명의 효과

[0018] 본 발명에 따른 효과는 다음과 같다.

[0019] 본 발명에서 제안하는 게임 이론을 이용한 보안 취약점 정량화 방법을 이용하면, 보안 취약점을 정량화 하고자 하는 대상 시스템의 보안 취약점을 객관적으로 산출할 수 있다. 또한, 공격자의 공격 경로와 공격 행동에 대한 대응 방안을 사전에 예측 및 대비할 수 있다.

[0020] 특히 게임 이론와 공격 트리를 이용하여 공격 경로를 트리 형태로 모델링 하고, 각 공격에 따른 공격자의 공격 비용과 방어자의 방어 비용 및 공격에 따른 영향력을 정량화할 수 있다. 정량화 된 분석 자료를 이용하면 어떠

한 유형의 공격을 더 중점적으로 예방하는 것이 좋은지에 대한 판단 기준을 제공할 수 있다. 이러한 과정을 통해 취약점을 사전에 분석하고 네트워크를 통한 공격으로부터 시스템을 안전하게 보호할 수 있다.

[0021] 본 발명의 효과들은 이상에서 언급한 효과들로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0022] 도 1은 본 발명의 일 실시예에서 사용되는 게임 이론과 공격 트리를 설명하기 위한 도면이다.

도 2는 본 발명의 일 실시예에 따른 게임 이론을 이용한 보안 취약점 정량화 방법을 개략적으로 설명하기 위한 도면이다.

도 3 내지 도 4는 본 발명의 일 실시예에 따른 게임 이론을 이용한 보안 취약점 정량화 방법의 한 단계인 게임 전략 모델링 과정을 설명하기 위한 도면이다.

도 5는 본 발명의 일 실시예에 따른 게임 이론을 이용한 보안 취약점 정량화 방법의 한 단계인 비용-영향 분석을 수행하는 과정을 설명하기 위한 도면이다.

도 6은 본 발명의 일 실시예에 따른 게임 이론을 이용한 보안 취약점 정량화 방법의 한 단계인 보상을 계산하는 과정을 설명하기 위한 도면이다.

도 7 내지 도 11은 본 발명의 일 실시예에 따른 게임 이론을 이용한 보안 취약점 정량화 방법을 도스 공격에 적용한 것을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0023] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0024] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0025] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0026] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0027] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0028] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0029] 도 1은 본 발명의 일 실시예에서 사용되는 게임 이론과 공격 트리를 설명하기 위한 도면이다.

[0030] 게임 이론은 원래 경제학 분야에 적용하기 위해 고안된 방법이나, 현재는 정치, 통신 기술, 전력 시스템 운영,

네트워크 보안 등 다양한 분야에서 사용되고 있다. 게임 이론에서 게임은 두 그룹 간의 전략적 상호 작용을 설명하고, 어느 한 그룹의 손익에 관한 상대 그룹의 전략적 선택의 효과를 분석하는데 사용된다.

[0031] 게임은 기본적으로 참여자(player), 행동(action), 보상(payoff)의 세 가지 요소로 구성된다. 게임 이론을 적용할 때 가장 중요한 두 가지 과정은 게임을 진행할 참여자를 구성하고, 각 참여자의 행동과 그 행동에 대한 보상을 결정하는 것이다.

[0032] 게임 이론을 네트워크 보안 분야에 적용하는 경우에, 참여자는 공격자와 이를 상대하는 시스템의 보안 관리자로 구성할 수 있다. 앞서 설명한 두 가지 과정 중 첫 번째 과정은 용이하게 적용이 가능하나, 시스템 구조, 네트워크 구성 환경 및 보안 제품 사용 여부와 같은 많은 변수가 고려되어야 하기 때문에 공격 행동과 이에 대응한 방어 행동의 객관적인 보상을 설정하는 두 번째 과정에는 많은 어려움이 있다.

[0033] 게임 모델의 신뢰성과 분석 결과의 타당성을 보장하기 위해서는 객관적이고 합리적인 기준을 사용하여 참여자의 행동의 효과를 계산하는 것이 매우 중요하다. 이를 위해서 본 발명에서는 게임 이론에 공격 트리를 적용해서 보안 취약점을 분석하는 방법을 제안하고자 한다.

[0034] 공격 트리(Attack Tree)는 네트워크를 통한 공격을 목록화 하고 이들의 순서를 표현하기 위한 방법이다. 공격 트리를 통해서 네트워크를 통한 공격자의 공격 시뮬레이션 시나리오를 작성할 수 있다. 또한, 네트워크 시스템의 보안 취약점을 정량화 하는데 사용될 수 있다.

[0035] 도 1을 참고하면, 공격 트리의 기본적인 형태가 도시되어 있다. 공격 트리는 네트워크 공격의 최종 목표를 루트 노드(root node)로 설정하고, 루트 노드가 그 아래에 다양한 하위 노드를 가지는 다중 계층 구조이다. 최종 목표인 루트 노드 아래에 세부적인 공격 목표를 하위 노드(child node)로 표시하여, 공격자의 가능한 공격 방법을 트리 형태로 모델링 할 수 있다.

[0036] 도 1을 참고하면, 공격자의 최종 목표는 당연히 대상 시스템의 오작동(System Failure)이다. 이를 달성하기 위한 방법으로 3가지 경로를 생각할 수 있다. 하나는 시스템에 조작된 메시지(fabricated message)를 전송하는 방법이며, 다른 하나는 시스템을 관리하는 직원을 속여 보안 정보를 탈취하는 수법, 즉 사회 공학(social engineering)의 방법이 있으며, 다른 하나는 서비스 거부 공격(Denial of Service attack)으로 흔히 도스 공격으로 알려진 방법이다.

[0037] 각각의 하위 노드는 해당 목표를 달성하기 위한 노드로 다시 분기가 가능하다. 조작된 메시지를 보내는 방법은 Halt Function, 즉 중단 메시지를 서버로 전송해서 오작동을 불러 있으키는 방법과 Loop Function, 즉 반복 메시지를 서버로 전송해서 서버가 다른 작업을 처리할 수 없도록 프로세스를 점유하는 방법으로 세분화 될 수 있다.

[0038] 도스 공격의 경우에는 분산 도스 공격, 일명 디도스 공격(DDoS)과 퍼머넌트 도스 공격, 일명 피도스 공격(PDoS)으로 나뉠 수 있다. 디도스 공격은 다수의 클라이언트에서 서버로 비정상적인 접속을 동시에 요청하여 다른 정상적인 요청을 처리할 수 없도록 하는 공격 방법이다. 피도스 공격은 네트워크를 기반으로 하는 펌웨어를 원격 업데이트 시킬 때 그 안에 악성 소프트웨어를 삽입시켜서 목표 시스템을 다운시키는 공격 방법이다.

[0039] 도 1에 예시한 공격 트리를 참고하면 네트워크 공격을 통해서 시스템을 다운 시킬 수 있는 다양한 시나리오를 접할 수 있다. 이때 트리의 각 노드는 하위 노트를 통해서 해당 목적을 달성하기 위한 각각의 보조 트리를 가지는 것을 볼 수 있다. 즉 앞서 설명한 다중 계층 구조를 확인할 수 있다.

[0040] 물론 도 1은 발명의 이해를 돕고자 예시한 것일뿐, 그 외에도 다양한 네트워크를 통한 공격 방법이 존재할 수 있다. 특이하게 도 1에서는 각각의 공격 방법 아래에 금액이 표시가 된 것을 볼 수 있다. 이는 공격자가 해당 공격을 수행하기 위해서 지불해야 하는 비용을 예시한 것이다. 이에 대해서는 추후에 보다 자세히 설명하기로 한다.

[0041] 도 2는 본 발명의 일 실시예에 따른 게임 이론을 이용한 보안 취약점 정량화 방법을 개략적으로 설명하기 위한 도면이다.

[0042] 앞서 우리는 게임 이론을 통해서 공격자와 방어자를 참여자로 가지는 게임을 모델링 했다. 게임 이론의 원리에 기초하여, 공격자는 네트워크 너머의 공격자이며, 그를 상대하는 방어자는 시스템의 보안 관리자이다. 이때 게임에 대한 추가적인 가정이 필요하다.

[0043] 우선 본 발명이 모델링한 게임은 두 명의 참여자가 경쟁하는 비협조적인 게임이며, 또한 각 참여자가 번갈아 가

며 진행하는 순차적인 게임이라고 가정한다. 그리고 본 발명에서 모델링한 게임은 각 참여자가 취한 행동을 정확히 알 수 있는 게임, 즉 완벽한 정보 게임(perfect information game)이라고 가정한다.

[0044] 이러한 가정 아래에서 본 발명에서 제안하는 시스템 보안 방법은 크게 3단계를 통해서 취약점을 분석한다. 도 2를 참고하면, 첫번째 단계에서 공격 행위의 도출(Accack Action Deduction)과 방어 행위의 도출(Security Action Deduction)을 수행한다. 적의 공격 행위를 식별하기 위해 공격 트리가 구성되어 적절한 단위로 그룹화된다. 방어 행위인 보안 조치의 경우, 보안 관리자는 식별된 공격 행동에 대응하기 위한 대응책을 결정한다. 이러한 과정을 통해 공격 시나리오에 따른 방어 시나리오가 마련된다.

[0045] 도 2를 참고하면, 두번째 단계에서 게임 이론을 기반으로 게임 전략 모델링(Game Strategy Modeling)이 수행된다. 모델링 프로세스는 공격자의 공격 활동과 보안 관리자의 보안 조치 사이의 상호 작용을 기반으로 수행된다. 루트 상태에서 시작하여 사용 가능한 공격 행동을 사용하여 분기 상태를 생성한다. 목표가 타협(compromise)되면 게임 전략 프로세스가 완료된다.

[0046] 그렇지 않으면 적용 가능한 보안 조치를 사용하여 분기 상태가 생성된다. 더 이상 가능한 공격 행동이 없으면 게임 전략 프로세스가 완료된다. 그렇지 않으면 수행할 수 있는 공격 행동이 남아있는 경우 게임 전략 모델링 프로세스가 계속된다. 이러한 과정을 통해서 공격자의 공격 시나리오와 방어자의 방어 시나리오를 시뮬레이션한다.

[0047] 도 2를 참고하면, 마지막인 세 번째 단계에서 비용-영향 분석(Cost-Impact Analyzation)을 수행한다. 이 단계를 통해서 각 행동의 비용이 계산되어, 각 행동에 따른 효과의 양을 계량화 할 수 있다. 그리고 각 행동의 효과는 비용을 포함한 각 행동의 특성을 기반으로 분석된다. 그리고 취약점 분석 대상 목표 시스템과 관련된 환경 요인을 고려하여 충격 값(impact value)을 결정한다. 마지막으로 목표 시스템의 보안 취약성은 각 상태마다 공격자와 보안 관리자의 보상(payoff)를 계산하여 계량된다.

[0048] 도 3 내지 도 4는 본 발명의 일 실시예에 따른 게임 이론을 이용한 보안 취약점 정량화 방법의 한 단계인 게임 전략 모델링 과정을 설명하기 위한 도면이다.

[0049] 게임 전략 모델링 중에 공격 및 보안 행동은 대상 시스템의 공격자와 보안 관리자 사이에 발생한다. 그리고, 상호 작용으로 인한 변화의 상태를 그래픽으로 표현하기 위해 트리 구조를 이용할 수 있다.

[0050] 여기서, 게임 전략 모델은 행동(action)과 상태(state)로 구성된다. 각각의 행동은 공격자 또는 보안 관리자가 수행할 수 있는 공격 또는 방어 중에서 어느 하나에 해당된다. 그리고 상태는 공격자와 보안 관리자의 행동을 기반으로 결과 상황을 나타낸다. 또한, 해당 상태에 대한 공격자 및 보안 관리자의 행동에 대한 성능 정보를 포함한다.

[0051] 게임 전략 모델을 구성하기 위해 '공격-보안 행동 도출'과 '반복적인 상태 생성'의 두 종류의 과정이 수행된다. 도 3을 참고하면, 공격 행동의 도출은 목표 시스템을 위해 설계된 공격 트리를 나타낸다. 공격 행동을 나타내는 하위 트리 그룹 단위로 공격 활동을 식별한다.

[0052] 도 3을 참고하면, 공격자의 공격 방법으로 A 공격 행동, B 공격 행동, C 공격 행동이 트리 형태로 도시되어 있다. 그리고, 공격 행동에 대한 응답으로 보안 행동의 도출을 위해 보안 관리자는 보안 장비 배포 및 네트워크 구성 변경과 같은 방어 방법을 목록화 한다.

[0053] 반복적인 상태 생성은 도 2에 설명되어 있으며, 이 과정에서는 루트 상태에서 사용할 수 있는 공격 행동에 의해 분기 상태가 생성된다. 후속 단계의 공격 행동은 이전 공격에 대응한 방어 행동을 통해 생성된다. 즉 공격자가 A라는 공격을 하면 이를 방어하기 위해 보안 관리자가 B라는 방어를 하고, 그러면 다시 공격자는 B라는 방어를 회피하기 위한 C라는 공격을 하는 방식이다. 이러한 방식으로, 게임의 상태를 확장하기 위해 공격-방어 행동이 반복되면, 도 4에 도시된 것과 같은 게임 전략 모델을 구성할 수 있다.

[0054] 도 4를 참고하면, 상태 A1에서 공격자의 공격 행동에 따라 상태 B1 내지 상태 B4으로 상태가 변경될 수 있다. 이에 대한 응답으로 방어자가 방어 행동을 취하면 다시 상태 C1 내지 상태 C8 중에 하나로 상태가 변경될 수 있다. 도 4에 대한 구체적인 예는 도 8에서 확인할 수 있다.

[0055] 특정 공격에 대한 방어자의 방어 행동에 따라 다음 상태에서 공격자가 취할 수 있는 공격 방법이 제한될 수 있다. 이를 통해 트리 구조로 공격 트리를 모델링하면서 공격자의 공격 시나리오와 방어자의 방어 시나리오를 매칭할 수 있다. 이렇게 게임 이론과 공격 트리를 이용하여 공격과 방어 과정을 모델링 한 후에는 각각의 상태에

대한 정량적인 평가가 필요하다.

[0056] 도 5는 본 발명의 일 실시예에 따른 게임 이론을 이용한 보안 취약점 정량화 방법의 한 단계인 비용-영향 분석을 수행하는 과정을 설명하기 위한 도면이다.

[0057] 본 발명에서는 비용-영향 분석과 같은 정량화 방법을 제안한다. 비용-영향 분석(Cost-impact analyzation)을 통해서 공격 행동과 방어 행동의 비용을 계산하고, 계산된 비용과 공격의 위험도를 기준으로 각 행동의 효과를 정량화하고, 분석 대상 시스템의 특징에 기초하여 행동의 영향을 계산한다. 도 5를 참고하면, 시스템의 보안 취약점을 계산하는데 사용되는 변수를 정의한 것을 볼 수 있다. 도 5에서도 볼 수 있듯이 본 발명에서는 정량화 과정을 위해 비용(cost), 효과(effect), 영향(impact)을 중점으로 비용-영향 분석을 수행한다.

[0058] 우선 비용을 계산하는 과정에서, 각 행동을 수행하는 데 필요한 비용은 공격 트리를 참조하여 계산된다. 공격자가 공격 행동을 수행하는데 필요한 비용은 공격 행동을 구성하는 공격 트리의 하위 트리에 있는 비용의 합계로 계산된다. 공격 행동에 대한 응답으로 보안 관리자가 취한 보안 행동의 경우 비용은 보안 장비를 적용하고 네트워크 구성을 변경하는 비용을 기반으로 계산된다. 이를 수학식으로 표현하면 다음의 수학식 1과 같다.

[0059] [수학식 1]

[0060] $$\text{cost}\,(a_i) = \sum cost\ (sub\_actions\ of\ a_i)$$

[0061] 물론 하위 노드가 없는 리프 노드의 경우에는 직접적으로 비용을 계산해서 산출해야 한다. 이 경우에는 공격자나 방어자가 해당 행동을 수행하기 위해서 필요한 인적 비용과 물적 비용 및 시간 비용을 고려할 수 있다. 예를 들면 (해당 행동을 취하는데 필요한 장비의 비용) + (인건비용/일) * (작업기간/일)과 같은 수식을 통해서 비용을 산출할 수 있다. 이렇게 산출된 비용은 공격 트리의 리프 노드에 입력될 수 있으며, 리프 노드의 상위 노드들은 앞서 설명한 것처럼 하위 노드의 비용의 합을 통해서 비용을 계산할 수 있다.

[0062] 다음으로 효과를 분석하는 과정에서, 공격 행동의 효과는 수학식 1에서 계산된 공격 행동의 비용뿐만 아니라 공격 행동의 성공 확률과 공격 행동의 위험도를 사용하여 정량화 할 수 있다. 일반적으로 더 높은 비용을 소모하는 공격 행동 또는 보안 행동은 높은 품질과 정밀도를 갖는다. 따라서 행동의 비용을 행동 효과의 정량화에 반영하는 것이다.

[0063] 공격 행동의 성공률 p는 0과 1 사이의 값을 갖진다. p의 값이 높을수록 수행된 공격으로 인해 피해를 입을 가능성이 커진다. 따라서 p가 높으면 공격의 효과가 더 커진다고 볼 수 있다. 공격 행동으로 인해 피해를 입힐 수 있는 위험도가 아무리 높더라도 성공 확률이 0%인 공격 행동은 의미가 없다는 점을 고려한 것이다.

[0064] 공격으로 인한 결과는 시스템이 구현되는 환경에 따라 다를 수 있다. 그래서, 공격 행동의 위험도는 0에서 10 사이의 값을 가지며 CVE(Common Vulnerabilities and Exposure)를 참조하여 설정할 수 있다. CVE는 공개적으로 알려진 소프트웨어의 보안취약점을 가리키는 고유 표기를 뜻한다. 공격 유형이나 사용된 기법, 공격 대상에 따라 공격 행동의 위험도가 다를 수 있다. 예를 들면 고위험 공격의 경우 공격의 효과가 크다.

[0065] 공격 행동의 효과를 비용과 성공 확률 및 위험도를 고려해서 정량화 하면 다음의 수학식 2와 같이 표현할 수 있다. 수학식 2를 참고하면, 위험도에 성공 확률을 지수승해서 비용에 곱한 값을 공격 행동의 효과로 정의할 수 있다.

[0066] [수학식 2]

[0067] $$effect\ (a_i) = cost\ (a_i) \times risk(a_i)^{p(a_i)}$$

[0068] 물론 위험도에 성공 확률을 지수승하지 않고 다른 방식으로도 수치화를 할 수 있다. 예를 들면 위험도에 성공 확률을 곱하는 것도 가능하다. 다만, 단순히 위험도에 성공 확률를 곱하는 연산을 하게 된다면, 이전 단계에서 산출되는 비용에 따라 효과 값 또는 영향 값이 1 이하로 작아질 수 있고, 만약 1 이하의 영향 값이 나오면 추후 방버 행동에 반영되는 람다 값을 계산할 때 log를 취하는 과정에서 음수 값이 나올 수 있다. 이러면 공격에 대한 부가 효과(side effect)로 방어자가 이득을 얻게 된다는 모순이 발생할 수 있기 때문에 지수승이 가장 바람직하다.

[0069] 공격 행동과 마찬가지로 보안 행동의 효과는 보안 관리자가 보안 행동을 수행하기 위해 소모한 비용, 성공 확률 및 이전에 수행된 공격 행동의 위험도를 이용하여 정량화 할 수 있다. 보안 관점에서 보았을 때 보안 행동의 효

과는 소모되는 비용이 높을수록, 보다 위험도가 높은 공격에 대응할수록 안전한 방어 행동으로 평가할 수 있기 때문이다.

[0070] 방어 행동의 효과를 비용과 성공 확률 및 위험도를 고려해서 정량화 하면 다음의 수학식 3와 같이 표현할 수 있다. 수학식 3을 참고하면, 방어 행동의 효과는 비용에 이전 공격 행동의 성공 확률을 지수승하고, 이전 공격 행동의 위험도를 곱해서 정량화 할 수 있다.

[0071] [수학식 3]

[0072] $$effect\ (a_i) = cost(a_i)^{p(a_{i-1})} \times risk\ (a_{i-1})$$

[0073] 서비스 거부(DoS) 공격은 기밀성 및 무결성보다 시스템의 가용성에 큰 영향을 미친다. 이처럼 적의 공격 행동과 이에 대응되는 보안 관리자의 방어 행동은 기밀성, 무결성 및 가용성에 각각 영향을 미치므로,기밀성, 무결성, 가용성 측면에서 가중치를 고려하여 각 행동의 영향을 분석할 수 있다.

[0074] 그런 다음 시스템에 대한 행동의 영향은 수학식 2와 3에 의해 계산된 공격자의 공격 효과와 방어자의 방어 효과에 결정된 가중치를 곱하여 정량화 할 수 있다. 기밀성, 무결성 및 가용성의 중요성은 취약점을 분석하고자 대상 시스템의 특성에 따라 다를 수 있으므로 가중치 역시 각각의 시스템에 따라 다르게 설정할 수 있다.

[0075] 예를 들어 가용성이 가장 중요한 보안 요소로 고려되는 전력 제어 시스템에서에서는 (기밀성, 무결성, 가용성)을 나타내는 가중치는 (0.2, 0.3, 0.5)과 같이 설정할 수 있다. 반면에 기밀성이 가장 중요한 보안 요소로 고려되는 소셜 IoT 환경의 경우, 가중치는 (0.4, 0.3, 0.3)과 같이 설정할 수 있다.

[0076] 이렇게 기밀성, 무결성, 가용성에 따라 가중치를 각각 설정한 후에 이를 합해서 전체의 가중치를 구할 수 있다. 다음의 수학식 4에서 wc는 기밀성(confidentiality)을 나타내는 가중치이며, wi는 무결성(integrity)을 나타내는 가중치이며, wa는 가용성(availability)을 나타내는 가중치이다.

[0077] [수학식 4]

[0078] $$w\ (a_i) = w_C + w_I + w_A\ (0 < w\ (a_i) \leq 1)$$

[0079] 이렇게 기밀성, 무결성, 가용성을 고려해서 구한 가중치에 앞서 계산한 효과를 곱하면 영향을 수치로 정량화 할 수 있다.

[0080] [수학식 5]

[0081] $$impact\ (a_i) = w\ (a_i) \times effect\ (a_i)$$

[0082] 도 6은 본 발명의 일 실시예에 따른 게임 이론을 이용한 보안 취약점 정량화 방법의 한 단계인 보상을 계산하는 과정을 설명하기 위한 도면이다.

[0083] 도 2에서도 볼 수 있듯이, 비용-영향 분석을 수행한 뒤 그 결과를 바탕으로 보상(payoff)를 계산한다. 보상을 계산하는 과정은 공격자와 방어자의 보상을 각각 계산한다. 이때 각각의 보상을 계산하는 수학식 6 내지 수학식 8이 도 6에 도시되어 있다.

[0084] 도 6을 참고하면, 공격 행동으로 인해 공격자는 수학식 6과 같이 많은 보상을 얻고, 방어자는 수학식 7과 같이 공격자가 얻는 보상의 음의 값을 보상으로 얻는다. 반대로 방어자의 방어 행동으로 인해 공격자는 얻는 보상이 없으나, 방어자는 수학식 8과 같은 보상을 얻는다.

[0085] 이때 수학식 6 내지 수학식 7에서 사용된 λi의 합은 수학식 9를 통해서 얻을 수 있다. 수학식 9를 참고하면 λi는 보안 관리자가 수행한 모든 방어 행동의 영향에 로그를 취한 값이다.

[0086] [수학식 9]

[0087] $$\lambda_i = log\ (Impact\ (a_i))\ , (i = 2, 4, 6, \ldots)$$

[0088] 예를 들어, 침입 탐지 시스템(IDS)이 네트워크 시스템에 배치되면 공격자의 공격 또는 비정상적인 행동을 쉽게 감지할 수 있다. 또한 설치된 보안 장비와 보안 관리자가 설정한 정책에 따라 시스템의 보안 수준이 향상될 수

있다. 이러한 방어자의 방어 행동을 누적해서 수학식 6 내지 수학식 8에서 영향(impact)에 더하거나 빼는 방식으로 정량화 할 때 반영하는 것이다. 이때 로그값을 취하는 이유는 게임 상태의 깊이(depth)가 진행됨에 따라 정량화 된 값들이 기하 급수적(exponential)으로 커질 수 있기 때문이다. 특히 람다 값은 영향 값에 따른 부수적인 효과이기 때문에 로그를 취해주어 작은 값으로 보정하는 것이 바람직하다.

[0089] 이상으로 본 발명에서 제안하는 게임 이론을 이용한 보안 취약점 정량화 방법에 대해서 살펴보았다. 본 발명에서 제안하는 게임 이론을 이용한 보안 취약점 정량화 방법은 게임 이론과 공격 트리를 이용하여 공격자의 공격 시나리오와 방어자의 방어 시나리오를 생성하고 각각의 행동에 소모되는 비용과 행동으로 인한 효과와 행동으로 인한 영향을 분석한다. 그리고 행동으로 인한 영향을 고려하여 공격자의 공격 행동과 방어자의 방어 행동에 대한 보상을 객관적으로 정량화 할 수 있다.

[0090] 도 7 내지 도 11은 본 발명의 일 실시예에 따른 게임 이론을 이용한 보안 취약점 정량화 방법을 도스 공격에 적용한 것을 설명하기 위한 도면이다.

[0091] 본 발명에서 제안하는 게임 이론을 이용한 보안 취약점 정량화 방법을 보다 자세히 살펴보기 위해 구체적으로 도스 공격에 대해서 이를 적용해보기로 한다. 구체적으로는 스마트 IoT 네트워크의 대표적인 사례인 스마트 홈 네트워크를 대상으로 한 도스 공격을 분석해본다.

[0092] 홈 네트워크는 다양한 가정용 IoT 기기, 각 기기의 전력 소비에 대한 정보를 표시하는 가정용 디스플레이(IHD; in-home display), 가정에서 에너지 소비를 제어하기 위한 고객 EMS, 고객 도메인 외부의 엔티티와 통신하기 위한 에너지 서비스 인터페이스(ESI; energy service interface), 통신 게이트웨이 역할을 하는 스마트 계량기 등을 포함한다.

[0093] 도스 공격에는 악의적인 기기 설치(installing rogue device), 설치된 장치의 손상(compromising installed device) 및 대상 기기의 방해(sabotaging the target)의 세 가지 종류의 공격 행동이 있을 수 있다. 이를 공격 트리로 표시하면 도 7과 같이 도시할 수 있다. 그리고 이에 대한 방어 행동으로, 장치의 구성을 변경하여 손상된 장치에 대응하고, 네트워크 구성을 변경하고, 설치된 악성 기기를 처리하기 위해 IDS를 적용하는 방법을 고려할 수 있다.

[0094] 공격 및 보안 행동을 참고하여 게임의 각 상태를 생성할 수 있다. 게임의 상태의 생성은 루트 상태에서 시작된다. 루트 상태의 하위 노드의 각 상태는 공격자의 공격 행동과 보안 관리자의 방어 행동 사이의 상호 작용에 의해 생성된다. 공격자가 공격 행동을 수행하기 시작하면 보안 관리자는 공격자의 공격에 대응되는 방어 행동을 취한다.

[0095] 방어 행동이 취해지면 새로운 분기 상태가 생성되어 하위 노드가 추가될 수 있다. 이렇게 해서 생성된 게임 전략의 모델은 도 8에 도시된 것과 같이 구성되며, 이 시나리오에서는 도스 공격이 홈 영역 네트워크(HAN)에 적용되어 가용성에 부정적인 영향을 미치는 경우를 기본 시나리오로 구성하였다. 도 8에서 1단계 상태는 공격으로 인해 생성된 상태이며, 2단계 상태는 방어로 인해 생성된 상태, 3단계 상태는 다시 공격으로 인해 생성된 상태이다.

[0096] 게임 상태를 생성한 후 각 행동의 정량화를 위해서 영향을 수치화 할 필요가 있다. 앞서 설명한 수학식 1, 2, 4 및 5를 통해서 도스 공격의 3가지 종류인 악의적인 기기 설치(installing rogue device), 설치된 장치의 손상(compromising installed device) 및 대상 기기의 방해(sabotaging the target)와 같은 공격 행동의 영향을 계산할 수 있다.

[0097] 그리고 이에 대한 대응으로 방어자의 방어 행동인 장치 구성 변경(changing device configuration), 네트워크 구성 변경(changing network configuration) 및 침입 탐지 시스템 적용(applying IDS)와 같은 방어 행동의 영향을 계산하기 위해 수학식 1, 3, 4, 5를 이용할 수 있다.

[0098] 이렇게 각각의 공격 행동의 영향과 방어 행동의 영향을 수치화 하는 과정에서 행동의 성공 확률, 행동의 위험도, 가중치가 필요한데 이는 각 행동 및 목표 시스템의 특성을 고려해서 설정한다. 본 실시예의 목표 시스템인 소셜 IoT 환경에서는 기밀성이 가장 중요한 보안 요소이므로 (기밀성, 무결성, 가용성)의 가중치는 (0.4, 0.3, 0.3)로 설정할 수 있다.

[0099] 공격자는 대상 시스템의 장치를 손상시킬 수 있다(compromising installed device). 이 행동의 정량화 된 효과 값은 수학식 2를 사용하여 계산된 14.3이다. 비용은 공격 트리에서 파생되며 위험과 확률은 CVE를 기반으로 설정할 수 있다. 장치가 손상되면 공격자는 기밀 정보를 얻을 수 있으며 부적절한 패킷이나 정보를 보낼 수 있다.

이러한 공격은 대상 시스템의 기밀성, 무결성 및 가용성에 영향을 준다. 따라서 이 공격 행동의 가중치는 1 (wc + wi + wa = 0.4 + 0.3 + 0.3)이고 영향은 동작의 효과와 동일한 14.3이다.

[0100] 공격자는 대상 시스템에 패킷 또는 조작 된 정보를 넘치게 하기 위해 불량 장치를 설치할 수 있다(installing rogue device). 이 행동의 정량화 된 효과 값은 수학식 2를 사용하여 계산된 35.8이다. 비용은 공격 트리에서 파생되며 위험과 확률은 CVE를 기반으로 설정할 수 있다. 이러한 공격은 대상 시스템의 무결성 및 가용성에 영향을 준다. 따라서 이 공격 행동의 가중치는 0.6(wi + wa = 0.3 + 0.3)이고 영향은 효과의 60%인 21.5이다.

[0101] 마지막으로 공격자는 대상 시스템의 전체 기능을 사용하지 못하도록 구성 요소를 방해하면서 가용성에 심각한 영향을 미칠 수 있다(sabotaging the target). 이 행동의 정량화 된 효과 값은 수학식 2를 사용하여 계산된 62.3이다. 비용은 공격 트리에서 파생되며 위험과 확률은 CVE를 기반으로 설정할 수 잇다. 이러한 공격은 대상 시스템의 가용성에만 영향을 미친다. 따라서 이 공격 행동의 가중치는 0.3 (wa = 0.3)이고 영향은 효과의 30%인 18.7이다.

[0102] 이러한 공격자의 공격 행동에 대응해서 방어자 역시 방어 행동을 취할 수 있다. 이를 정량화 하면 다음과 같은 결과를 얻을 수 있다.

[0103] 보안 관리자는 설치된 장치의 손상(compromising installed device)의 공격에 대한 대응으로 공격받은 장치의 구성을 변경할 수 있다(changing device configuration). 이렇게 하면 공격자가 손상된 장치를 제어하거나 접근하는 것을 막을 수 있다. 이러한 방어 행동의 정량화 된 영향 값은 수학식 3 내지 수학식 5를 사용하여 계산된 8.3이다. 위험 요소, 확률 및 가중치는 설치된 장치의 손상(compromising installed device)이라는 공격 행동의 값을 기반으로 한다. λ의 값은 수학식 9에 의해 계산된 2.1이다.

[0104] 또한 보안 관리자는 악의적인 기기 설치(installing rogue device)의 공격에 대한 대응으로 네트워크 설정을 재구성 할 수 있다(changing network configuration). 이를 통해서 악의적인 기기가 네트워크에 프로비저닝하거나 참여하거나 HAN(home area network)에 접근하는 것을 방지할 수 있다. 이러한 방어 행동의 정량화 된 영향 값은 수학식 3 내지 수학식 5를 사용하여 계산된 9.5이다. 마찬가지로 위험 요소, 확률 및 가중치는 악의적인 기기 설치(installing rogue device)라는 공격 행동의 값을 기반으로 한다. λ의 값은 수학식 9에 의해 계산된 2.3이다.

[0105] 그리고, 보안 관리자는 침입 탐지 시스템을 적용하여 네트워크에서 비정상적인 동작을 탐지하고 네트워크에서 차단할 수 있다(applying IDS). 이러한 방어 행동의 정량화 된 영향 값은 수학식 3 내지 수학식 5를 사용하여 계산된 16.7이다. 마찬가지로 위험 요소, 확률 및 가중치는 악의적인 기기 설치(installing rogue device)라는 공격 행동의 값을 기반으로 한다. λ의 값은 수학식 9에 의해 계산된 2.8이다.

[0106] 도 9 내지 도 10은 스마트 홈 네트워크의 보안 취약성을 수치화하는데 필요한 수치를 나열한 것이다. 각각의 공격 행동과 방어 행동의 정량화 된 영향 값을 사용하여 그림 11과 같이 게임 전략 모델의 각 상태에서 공격자와 방어자의 보상(payoff)를 계산할 수 있다.

[0107] 상태에 표시된 값 (x, y)는 각각 공격자의 보상 x와 방어자의 보상 y를 나타낸다. 이러한 정량화 된 결과를 통해서 보안 관리자가 적의 공격에 대해 적절한 조치를 취하는데 도움이 될 수 있다.

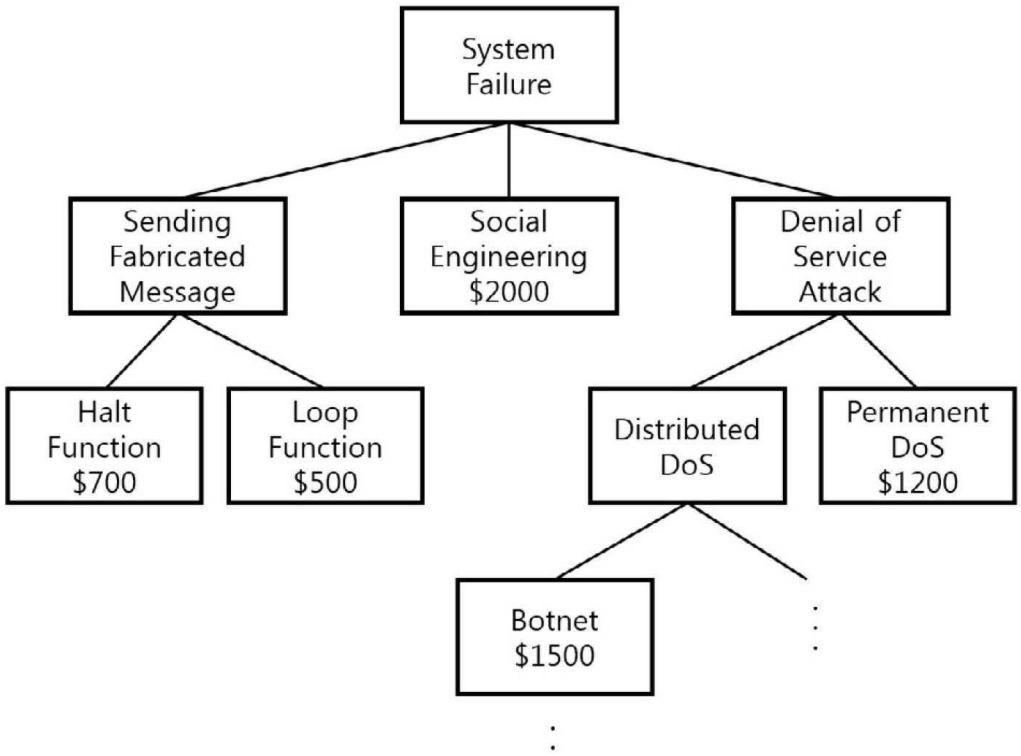
[0108] 예를 들어, 악의적인 기기 설치(installing rogue device)라는 공격에 대응해서 침입 탐지 시스템을 적용(applying IDS)해서 방어를 했다고 가정해보자. 그러면 루트 노드에서는 보상이 (0, 0)에서 공격자가 악의적인 기기를 설치한 후에는 보상이 (21.5, 21.5)로 변경된다. 이 상태에서 침입 탐지 시스템을 적용하면 보상은 (21.5, -2.0)으로 변경된다. 이 상태에서 공격자가 재차 목표 시스템을 방해하는 공격을 수행하면(sabotaging the target) 해당 상태의 보상은 (37.4, -17.9)로 변경되는 것을 볼 수 있다.

[0109] 이렇게 각 상태별로 공격자의 보상과 방어자의 보상을 계산하면 이를 통해서 사전 대응을 취하는데 우선 순위를 세울 수 있다. 예를 들면, 보상의 절대값이 큰 경우를 1순위로 하여 사전 대응을 취할 수 있다. 또는 게임 상태의 깊이(depth)간 보상(payoff)의 차이가 큰 경우를 2순위로 하여 사전 대응을 취할 수 있다.

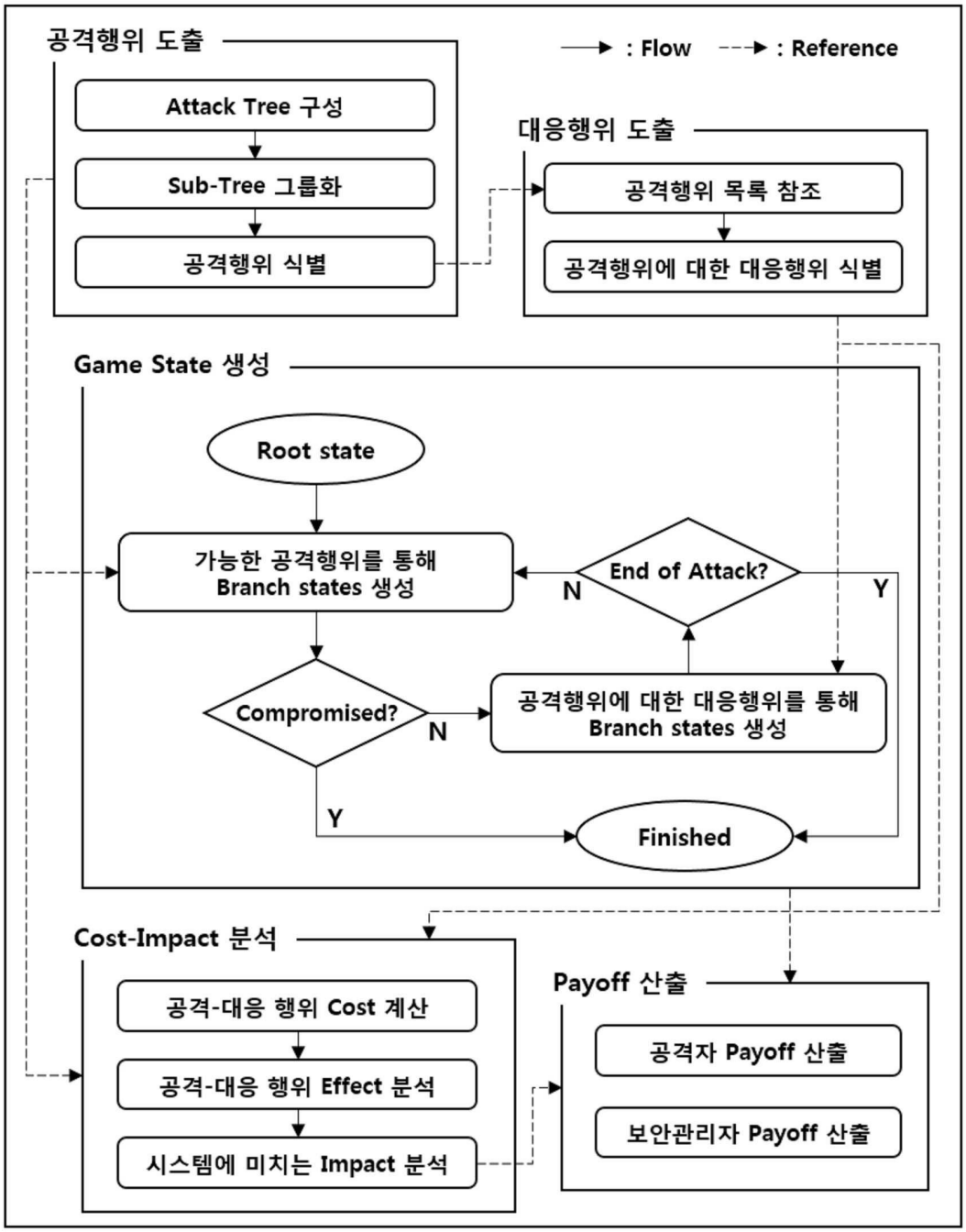
[0110] 이상 첨부된 도면을 참조하여 본 발명의 실시 예들을 설명하였지만, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시 예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다.

도면

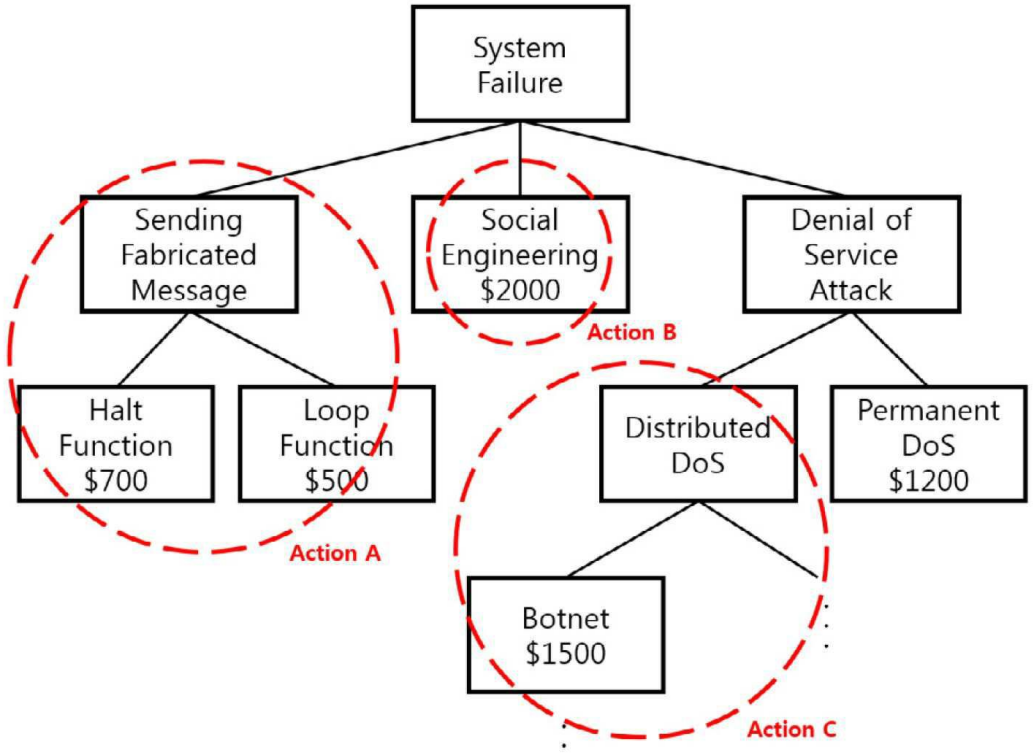
도면1


System Failure
Sending Fabricated Message
Social Engineering $2000
Denial of Service Attack
Halt Function $700
Loop Function $500
Distributed DoS
Permanent DoS $1200
Botnet $1500

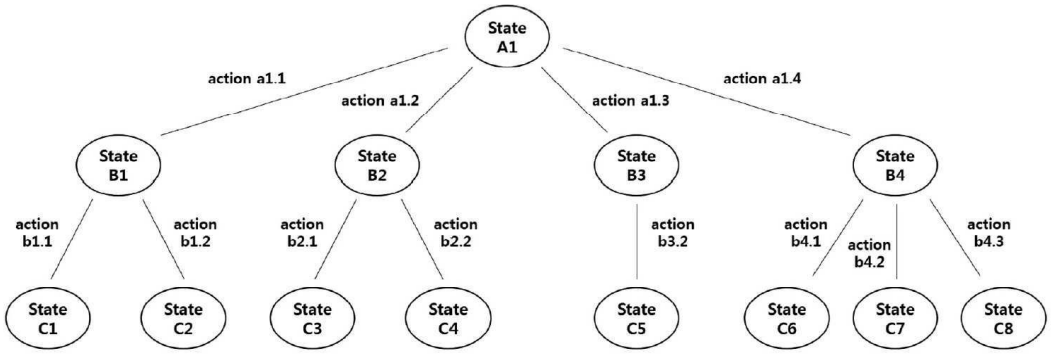
도면2


공격행위 도출
: Flow
: Reference
Attack Tree 구성
Sub-Tree 그룹화
공격행위 식별
대응행위 도출
공격행위 목록 참조
공격행위에 대한 대응행위 식별
Game State 생성
Root state
가능한 공격행위를 통해
Branch states 생성
End of Attack?
N
Y
Compromised?
N
공격행위에 대한 대응행위를 통해
Branch states 생성
Y
Finished
Cost-Impact 분석
공격-대응 행위 Cost 계산
공격-대응 행위 Effect 분석
시스템에 미치는 Impact 분석
Payoff 산출
공격자 Payoff 산출
보안관리자 Payoff 산출

도면3



도면4



도면5

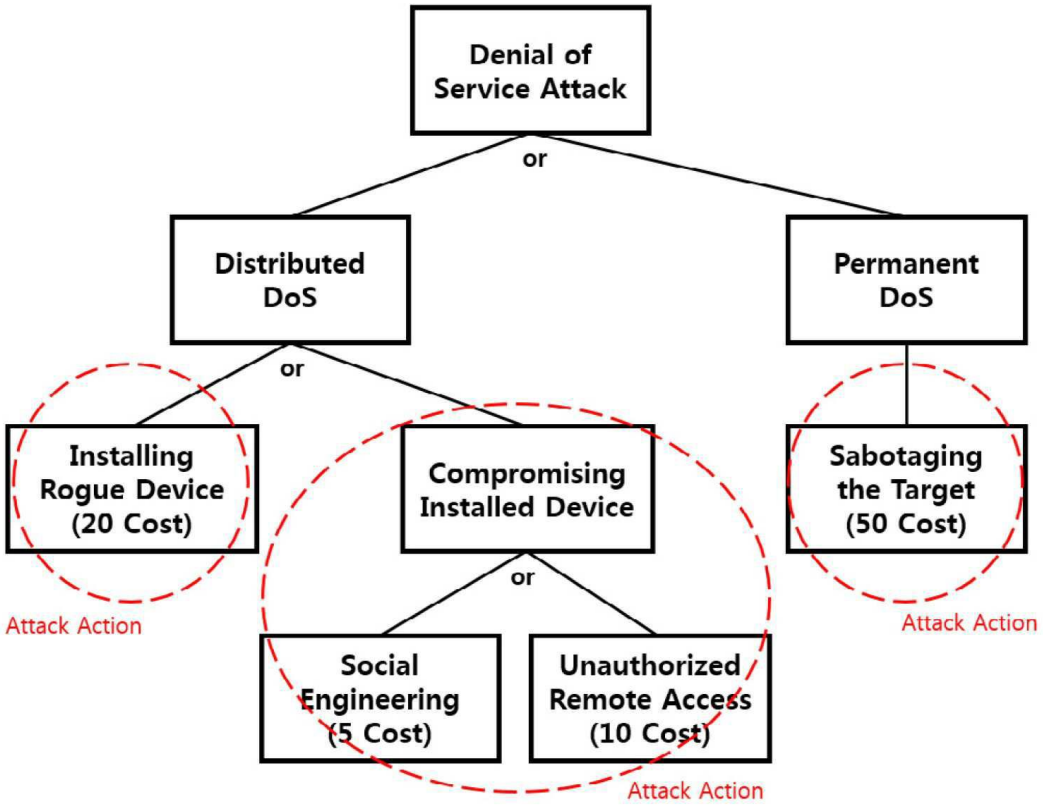
Variables	Meaning
$cost$	required cost to perform an action
a_i	an action performed at i^{th} depth
$risk$	risk of an attack action
p	attack action's probability to succeed
$effect$	quantified effect of the action
w	weight vector related to security factor
$impact$	action's quantified impact on the system

도면6

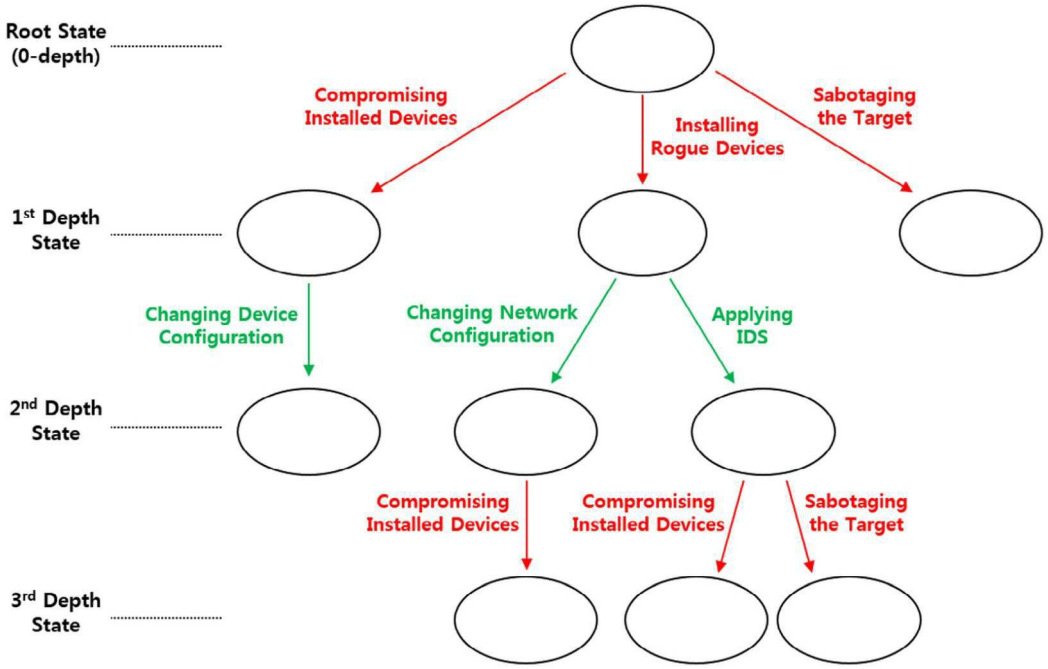
	Adversary's action	
Payoff of adversary	$Impact\ (a_i) - \sum_{j=0}^{i-1}\lambda_j$	(6)
Payoff of security administrator	$-Impact\ (a_i) + \sum_{j=0}^{i-1}\lambda_j$	(7)

	Security administrator's action	
Payoff of adversary	-	
Payoff of security administrator	$Impact\ (a_i) + \lambda_i$	(8)

도면7



도면8



도면9

Quantification of attack actions.

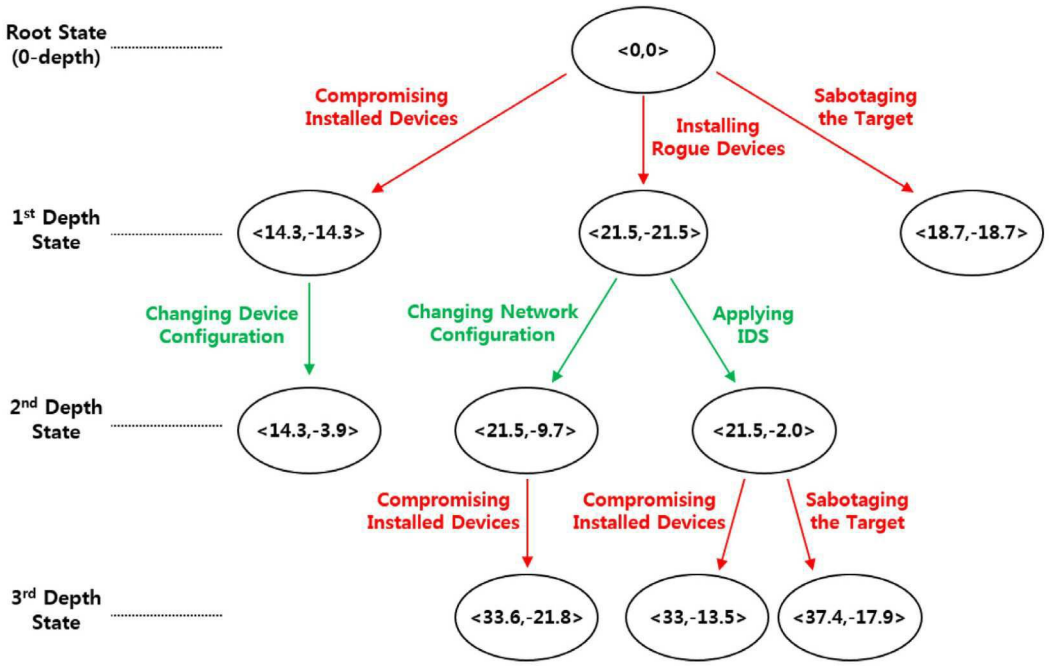
Action	Cost	Risk	p	Effect	w_C	w_I	w_A	Impact
Compromising Installed Device	10	6	0.2	14.3	0.4	0.3	0.3	14.3
Installing Rogue Device	20	7	0.3	35.8	0	0.3	0.3	21.5
Sabotaging the Target	50	9	0.1	62.3	0	0	0.3	18.7

도면10

Quantification of security actions.

Action	Cost	Risk	p	Effect	w_C	w_I	w_A	Impact	λ
Changing device configuration	5	6	0.2	8.3	0.4	0.3	0.3	8.3	2.1
Changing network configuration	15	7	0.3	15.8	0	0.3	0.3	9.5	2.3
Applying intrusion detection system	100	7	0.3	27.9	0	0.3	0.3	16.7	2.8

도면11


Root State
(0-depth)
<0,0>
Compromising
Installed Devices
Installing
Rogue Devices
Sabotaging
the Target
1st Depth
State
<14.3,-14.3>
<21.5,-21.5>
<18.7,-18.7>
Changing Device
Configuration
Changing Network
Configuration
Applying
IDS
2nd Depth
State
<14.3,-3.9>
<21.5,-9.7>
<21.5,-2.0>
Compromising
Installed Devices
Compromising
Installed Devices
Sabotaging
the Target
3rd Depth
State
<33.6,-21.8>
<33,-13.5>
<37.4,-17.9>