한국시뮬레이션학회 논문지
Vol. 21, No. 3, pp. 17-24 (2012. 9)
http://dx.doi.org/10.9709/JKSS.2012.21.3.017

시뮬레이션을 이용한 DDoS공격 대응기술 효과성평가방법

김애찬[1] · 이동훈[1] · 장성용[2†]

The Effectiveness Evaluation Methods of DDoS Attacks Countermeasures Techniques using Simulation

Ae-Chan Kim · Dong-Hoon Lee · Seong-Yong Jang

ABSTRACT

This paper suggests Effectiveness Evaluation Methods of DDoS attacks countermeasures model by simulation. According to the security objectives that are suggested by NIST(National Institute of Standards and Technology), It represents a hierarchical Effectiveness Evaluation Model. we calculated the weights of factors that security objectives, security controls, performance indicator through AHP(Analytic Hierarchy Process) analysis. Subsequently, we implemented Arena Simulation Model for the calculation of function points at the performance indicator. The detection and protection algorithm involve methods of critical-level setting, signature and anomaly(statistic) based detection techniques for Network Layer 4, 7 attacks. Proposed Effectiveness Evaluation Model can be diversely used to evaluate effectiveness of countermeasures and techniques for new security threats each organization.

Key words : DDoS, Simulation, Security Objectives, Security Controls, AHP, Effectiveness Evaluation

요 약

본 논문은 시뮬레이션을 이용한 DDoS공격 대응기술의 효과성을 평가하기 위한 방법을 제시한다. 미국 국가표준기술연구소(NIST: National Institute of Standards and Technology)에서 제시한 보안목표에 따라 효과성평가모형을 계층적으로 표현하였다. 보안목표, 보안통제, 성과지표에 해당하는 요인들의 가중치 계산을 위해 계층적 분석(AHP: Analytic Hierarchy Process)을 적용하고, 최하위계층인 성과지표의 기능점수계산을 위해 Arena시뮬레이션모델을 구현하였다. 탐지 및 차단 알고리즘은 네트워크 L4, L7계층 공격에 대한 임계치설정, 시그니쳐기반탐지, 행동(통계)기반탐지 기술을 복합적으로 검증하였다. 제안된 효과성평가모형은 조직마다 상이한 보안목표와 위협에 따라 다르게 설계될 수 있으므로 새로운 보안위협에 대한 대응방안이나 대응기술의 효과성을 평가할 수 있는 방법으로 활용될 수 있다.

주요어 : 디도스, 시뮬레이션, 보안목표, 보안통제, AHP, 효과성평가

1. 서 론

2009년 7월 7일 공공기관 및 금융회사 등을 대상으로 한 DDoS공격으로 사회적 관심이 고조된 이후 정보보호 유관기관 및 보안전문업체의 DDoS공격에 대한 대응기술들이 많은 부분 연구되었다. 그러나 대부분의 연구는 실질적인 DDoS공격 대응기술의 검증과 평가를 위해 실제와 유사한 실험환경을 제공해야 했으므로 이를 위한 많은 시간과 비용이 소요되었다. 최근의 DDoS공격규모와 방법은 들어 더욱 대규모, 다양화되는 추세를 보이며[6], 네

*이 논문은 지식경제부와 한국인터넷진흥원의 『고용계약형 지식정보보안 석사과정』지원을 받아 수행되었습니다. (No. H2101-12-1001).
접수일(2012년 6월 5일), 심사일(1차 : 2012년 9월 4일), 게재 확정일(2012년 9월 11일)
[1] 고려대학교 정보보호대학원
[2] 서울과학기술대학교 글로벌융합산업공학과
주 저 자 : 김애찬
교신저자 : 장성용
E-mail; syjang@seoultech.ac.kr

트워크에서 대용량데이터처리의 문제와 함께 DDoS공격에 대한 대응은 근본적으로 해결하기가 매우 어려운 수준의 위협에 직면하고 있다.

이명수 등(2010)은 DDoS공격 대응장비의 한계용량을 계산하는 방법을 정립하여 정량적 분석이 가능한 DDoS 대응 체계를 수립하여 한국인터넷진흥원에서 운용하고 있는 사이버대피소 구축에 기여하였다는 긍정적인 평가를 받으나 기술적 분석에 중점을 두었다는 한계를 갖는다[3]. 김지연 등(2009)은 네트워크의 흐름을 OPNET시뮬레이터로 구현하여 비용을 산정하는 모델링방법을 제안하였지만 보다 다양하게 변형되고 있는 현재의 DDoS공격과 대응기술에 대한 시뮬레이션 검증이 부족하다[1]. 김태원 등(2010)은 DDoS공격 발생 시 유입되는 패킷의 개수를 카운팅하고 효율적으로 탐지하기 위한 판별 알고리즘을 제안하였다[2]. 또한, 장범수 등(2010)은 전송되는 공격 패킷의 수는 미탐율(false negative rate)에 비례하며 전송되는 일반 패킷의 수는 일정치 이하의 미탐율과 오탐율(false positive rate)에 반비례한다는 연구결과를 제시함으로서 대응기술의 탐지 알고리즘 성능개선의 중요성을 역설하였다[5].이진수 등(2009)은 DDoS에 대한 임계값 알고리즘에 근거한 3단계 탐지 알고리즘을 제안하였고, 사이버테러 대응시스템에 적용하여 알고리즘을 검증하였다. 하지만 제안된 알고리즘은 L4기반 공격만 검증이 가능하였다는 점에 한계가 있었다[4].

Jie Wang et al.(2011)은 Spirent Test Center에서 DDoS 트래픽과 정상 트래픽을 동시에 발생시켜 DDoS탐지 및 차단기술을 테스트할 수 있는 테스트베드(testbed)기반 시뮬레이션 방법을 제안하였다. 그러나 별도의 하드웨어 플랫폼을 이용해야하고 단순한 L4기반 DDoS공격방법으로만 실험하였다는 점에 한계가 있다[9]. Nidal et al.(2011)은 오픈소스 Oversim 시뮬레이터를 이용하여 P2P기반 네트워크 DDoS공격 실험을 하였다. 이 논문은 노드 간 연결된 네트워크의 대역폭이 고갈되는 과정을 단계적으로 실험함으로써 특정 노드에 대한 성능저하와 인접 노드 및 전체 네트워크의 성능저하 확산문제를 제기하였다[11].

본 논문에서는 논문 [2]와 논문 [4]에서 제안된 DDoS 대응 탐지알고리즘을 기초로, 현재 현장에서 변용중인 탐지 및 차단 알고리즘을 시뮬레이션에 반영함으로써 DDoS대응 장비 구입 및 서비스 도입 시 고려사항으로 활용될 수 있는 효과성평가모형을 제안한다. 효과성평가모형은 조직의 정보보안 보증수준(Assurance Level)으로 요구되는 보안목표와 그에 상응하는 보안위협에 대한 대응방안, 또는 기술에 대한 효과성을 평가할 수 있는 기능점수계산방법이다. 이것은 보안목표에 따라 달리 수립될 수 있는 효과성평가모형이며, 궁극적으로 AHP분석[13]과 Arena 범용시뮬레이터의 구현으로 어떻게 대응기술의 효과성을 평가할 수 있는지 설명한다.

2. 효과성평가모형

2.1 효과성평가모형 설계

본 논문에서 효과성을 평가하기 위한 계층화모형은 그림 1과 같다. 최상위계층인 보안목표는 NIST에서 제안하는 기준[10]에 따라 분류하였다. 보안목표는 조직이 특정 보안위협에 대해 허용 가능한 범위내로 위험을 완화하기 위해 보증되어야 하는 요인을 말한다.

그림 1의 모형에서 DDoS공격에 상응하는 보안위협은 '웹서버의 지속가능한 서비스지원불가'이기 때문에 보안목표를'가용성'에 한정하였고, 가용성의 차상위계층인 보안통제영역을 3가지 - 관리적(Administrative), 기술적(Technical), 물리적(Physical)[8]통제 - 로 분류하였다. 관리적통제영역에서 제품과 서비스 '적합성' 지표의 요인으로 고객의 만족도와 관련된 '서비스/제품 품질점수'로 정의하였으나[12], 본 논문에서는 범위를 벗어나므로 다루지 않는다. 기술적통제영역에서 성과측정을 위한 지표(performance indicator)로 대응기술의 하드웨어 동작특성인 '신뢰성'과 소프트웨어 기능특성인 '정확성'으로 분류하였다. '신뢰성'지표는'가용도 점수'로 정의하고, '정확성'지표는 '탐지 정확도점수'로 정의하였다. 물리적통제영역에서 시설 및 소프트웨어에 대한 접근통제 정확도를 평가할 수 있으나 이 또한 본 논문의 범위를 벗어나므로 다루지 않는다.

만약 조직이'기밀성'보증이라는 보안목표를 요구할 때

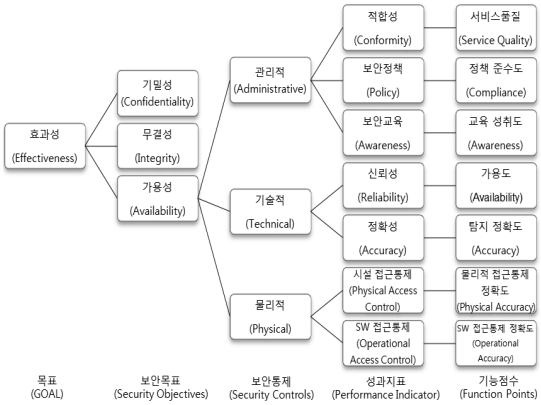

그림 1. DDoS공격 대응기술 효과성평가 계층화모형

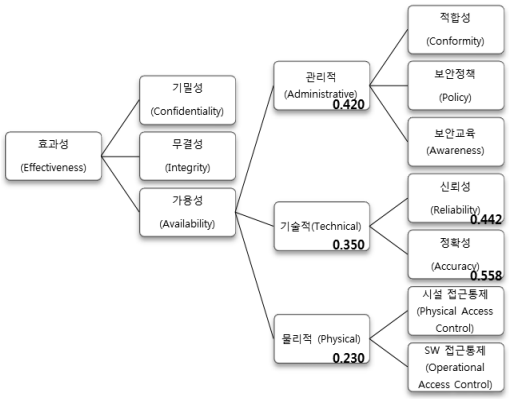

그림 2. DDoS공격 대응기술의 AHP분석결과

에는'기밀성'의 하위요인으로서 보안통제영역 요인을 계층화하여 각 보안통제영역의 하위요인을 재분류할 수 있다(예1: 효과성평가-기밀성-물리적-(시설||SW)접근통제-(물리적||SW)접근통제 정확도, 예2: 효과성평가-기밀성-관리적-{(적합성-서비스품질)||(보안정책-정책준수도)||(보안교육-교육성취도)}).

2.2 AHP분석을 통한 요인의 가중치산정

그림 1에서 수립된 DDoS공격 대응기술 성과지표의 가중치 산정을 위해 AHP분석으로 보안전문업체 보안관제/CERT업무를 맡고 있는 현업담당자 25명을 설문하여 분석한 결과는 그림 2와 같다. AHP분석결과의 신뢰도를 판단하는 기준인 CR(Consistency Rate)의 값이 0.1보다 낮으므로(CR = 0.06) 분석은 유효한 것으로 확인되었다. DDoS공격 대응에 보안목표인'가용성'의 예하 요인으로 보안통제(2계층)영역에서 관리적요인(0.420), 기술적요인(0.350), 물리적요인(0.230)의 순으로 중요하게 생각하는 것으로 나타나, 관리적·기술적통제가 물리적통제에 비해 DDoS공격 대응에 있어 중요한 요인으로 생각되는 것으로 확인되었다. 기술적통제 성과지표(3계층)는 대응장비의 정확성지표(0.558)가 신뢰성지표(0.442)보다 더 중요한 요인으로 생각되는 것으로 확인되었다.

2.3 DDoS공격 대응기술 평가모형

본 논문에서는 DDoS공격 대응기술의 효과를 정량적으로 평가하고 시뮬레이션 결과를 반영할 수 있는 기능점수 계산방법을 제안한다. 기능점수계산과 관련하여 사용되는 기호를 다음과 같이 정의한다.

[Notation]

EP: 효과성평가점수

α: 보안목표(기밀성), C: 기밀성점수

β: 보안목표(무결성), I: 무결성점수

γ: 보안목표(가용성), A: 가용성점수

$W_\alpha, W_\beta, W_\gamma$: 기밀성, 무결성, 가용성가중치

$$\alpha, \beta, \gamma = \begin{cases} 1, & \text{보안목표를 반영함} \\ 0, & \text{보안목표를 반영하지 않음} \end{cases}$$

$\gamma_1, \gamma_2, \gamma_3$: 가용성목표와 관련된 보안통제(관리적, 기술적, 물리적)요인

$$\gamma_1, \gamma_2, \gamma_3 = \begin{cases} 1, & \text{보안통제요인을 반영함} \\ 0, & \text{보안통제요인을 반영하지 않음} \end{cases}$$

$W_{\gamma_1}, W_{\gamma_2}, W_{\gamma_3}$: 가용성목표와 관련된 관리적, 기술적, 물리적통제요인의 가중치

γ_{21}, γ_{22}: 기술적통제와 관련되어 시뮬레이션으로 측정된 장비 가용도 점수(%), 탐지 정확도 점수(%)

$W\gamma_{21}, W\gamma_{22}$: 기술적통제와 관련된 신뢰성, 정확성가중치

N: 시스템으로 유입된 모든 패킷 수(정상 패킷과 DDoS 공격패킷 혼합)

P: DDoS대응장비가 DDoS공격패킷으로 탐지하여 차단하는 패킷 수

$$DR(\text{Defense Rate, 패킷차단율}) = \frac{\sum_{t=1}^{n} P_t}{\sum_{t=1}^{n} N_t}(\%)$$

DDoS공격 대응기술의 효과성을 정량화하기 위해서 먼저 각 조직에서 보증하고자하는 보안목표를 반영해야 한다. 마찬가지로 $\gamma_1, \gamma_2, \gamma_3$는 가용성점수계산을 위해 가용성목표와 관련된 3가지 보안통제영역을 반영할 것인지의 여부를 의미한다. 즉, 값이 '1'인 경우에는 요인이 반영되어 계산되며, 값이 '0'인 경우에는 요인이 반영되지 않는다. 본 논문에서는 가용성에 한정하였으므로 식 (1)에서 $\alpha, \beta = 0$, $\gamma = 1$이다.

$$EP = (\alpha \times W_\alpha) + (\beta \times W_\beta) + (\gamma \times W_\gamma) = C + I + A \qquad (1)$$

본 모형에서는 가용성점수 계산을 위해 AHP분석결과로 산정된 가용성목표와 관련된 보안통제요인의 가중치($W\gamma_1 = 0.420$, $W\gamma_2 = 0.350$, $W\gamma_3 = 0.230$)를 고정 값으로 할당할 수 있으나 기술적통제요인을 반영하고, 관리적, 물리적통제요인은 반영하지 않았으므로 식 (2)에서 $\gamma_2 = 1$, $\gamma, \gamma_3 = 0$이다.

$$A=(\gamma_1\times W_{\gamma_1})+(\gamma_2\times W_{\gamma_2})+(\gamma_3+W_{\gamma_3}) \quad (2)$$

또한, 기술적통제점수 계산을 위해 AHP분석결과로 산정된 기술적통제와 관련된 신뢰성과 정확성가중치 ($W_{\gamma_{21}}=0.442$, $W_{\gamma_{22}}=0.558$)를 고정 값으로 할당할 수 있다. 또한, 식 (3)과 식 (4)에서 γ_{21}, γ_{22}는 Arena시뮬레이션으로 측정될 수 있는 기능점수(%)가 된다.

$$\gamma_{21}=\frac{MTBF}{MTBF+MTTR}\text{[1)]}, \text{ (장비 가용도(\%))} \quad (3)$$

$$\gamma_{22}=1-(DR), \text{ (탐지 정확도(\%))} \quad (4)$$

제안된 평가모형은 이해관계자들의 가중치가 반영된 것이며, 또한 DDoS대응기술의 알고리즘이나 논리가 정량적인 방법으로 설계가 가능할 때 탐지 알고리즘 정확도와 장비 가용도의 성능을 측정하기 위해 Arena시뮬레이터를 이용할 수 있다. 만약 정량적인 방법으로 측정이 불가능하고 탐지 알고리즘이나 논리가 구현이 어려운 경우에는 시뮬레이션 측정과정을 생략하여 효과성을 평가하는 것도 고려될 수 있다.

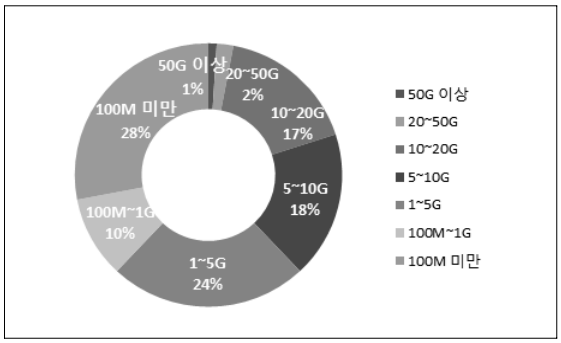

그림 3. 2011년 DDoS공격량 규모

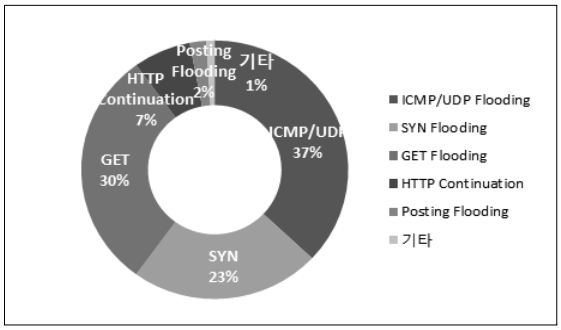

그림 4. 2011년 DDoS공격유형별 빈도

3. 실험 및 결과분석

3.1 DDoS공격유형 및 동향

2011년 발생한 DDoS공격량 규모는 5 Gbps 이상이 전체의 37%를 차지하며, 비교적 유효한 규모의 DDoS 공격이라 할 수 있는 100 M～5 Gbps의 공격규모는 51%를 차지한다. 그 밖에 미비한 공격이라 할 수 있는 100Mbps 미만의 공격은 전체의 28%정도를 차지한다(그림 3)[6].발생한 공격유형을 살펴보면 ICMP, UDP, SYN Flooding과 같은 고전적 형태의 L3-4 Layer기반공격이 전체 61%를 차지하고 있다. 또한 L7기반의 GET, POST Flooding, HTTP Continuation과 같은 공격도 나머지 39%를 차지한다. 현재까지도 앞서 언급한 고전적인 공격들이 가장 많이 발생하고 있지만, 최근에는 특정 목표를 대상으로 하는 L7기반 공격이 점차 늘어나고 있다. CC Attack이 대표적인 공격기법이다(그림 4)[6].

본 논문에서는 대표적 공격유형인 L4 UDP Flooding과 L7 CC Attack[2)], GET Flooding(Slowloris)에 대한 시뮬레이션결과를 평가에 반영하였다.

3.2 탐지 및 차단 알고리즘

침입탐지시스템(IDS: Intrusion Detection System)은 데이터 수집위치와 탐지방식에 따라 분류할 수 있는데, 본 논문에서는 네트워크상에서 발생하는 문제만을 다루므로 호스트기반 침입탐지시스템(H-IDS)은 다루지 않는다. 표 1에서 침입탐지시스템은 탐지방식에 따라 오용(Misuse)탐지방식과 이상(Anomaly)탐지방식으로 분류된다. 시그니쳐기반 탐지기술은 유입되는 파일이나 패킷의 헤더(header)를 탐지규칙으로 설정해 놓은 시그니쳐와 비교하는 기술을 의미하며, 행동기반 탐지기술은 유입되는 패킷의 통계량을 근거로 패턴을 찾아내는 기술을 의미한다[7].

현재 DDoS대응장비를 판매하는 업체별로 채택하는 기술과 사용방법이 조금씩 상이하나 차용되어 사용 중인

1) MTTR(평균수리시간, Mean Time To Repair): 수리 시간의 평균치, MTBF(평균고장간격, Mean Time Between Failure): 수리할 수 있는 설비의 고장에서부터 다음 고장까지 동작시간의 평균치

2) HTTP의 user-agent속성에 Cache-Control부분을 임의로 수정하여 서버로 부터 받은 데이터를 client cache에 저장하지 않고 계속 적으로 요청하여 서버에 부하를 주는 공격

표 1. 탐지방식에 따른 침입탐지시스템 분류

	오용탐지 (Misuse Detection)	이상탐지 (Anomaly Detection)
동일용어	시그니쳐기반, 지식기반	행동(통계)기반
탐지방법	시그니쳐(패턴매칭)	임계치 초과, 패턴인식
적용원리	전문가 시스템 (IF / THEN rule-based)	인공지능, 데이터마이닝
장점	낮은 오탐율	Zero-day Attack탐지가능
단점	알려진 공격만 탐지, 시그니쳐 업데이트 필요	높은 오탐율

표 2. DDoS공격 대응 전용장비

제조 회사	윈스테크넷	시큐아이닷컴	라드웨어	인트루가드
제품명	Sniper DDX	SECUI NXG 4000D	Defense Pro	IG 2000
기반 기술	IPS	NBA	L7 Switch	NBA
성능	4/12Gbps, 6만 CPS, 4/8GB	4Gbps, 20만CPS, 4/8GB	4Gbps, 20만CPS, 4/8GB	2Gbps, 4/8GB
구성 방식	In-line / Out of Path	In-line / Out of Path	In-line	In-line
L4 방어	임계치	임계치 / 행동기반	임계치	임계치 / 행동기반
L7 방어	시그니쳐 (Misuse)	행동기반 (Anomaly)	시그니쳐 (Misuse)	행동기반 (Anomaly)

탐지 알고리즘은 크게 다르지 않다. L4대응방법에는 주로 시그니쳐기반 탐지기술과 임계치(Critical Level)설정에 근거한 행동기반 탐지기술을, L7대응방법으로는 시그니쳐기반 탐지기술과 행동기반 탐지기술을 선택하여 적용하고 있다(표 2)[3].

3.3 시뮬레이션 모델

대응기술의 기능점수(γ_{21}, γ_{22})를 장비 가용도 점수와 패킷차단율로 측정하고자할 때 Arena시뮬레이터로 구현된 모형은 그림 5와 같다. 모델은 패킷 생성 부분과 대응기술 부분이 통합된 형태로 구현된다[4]. 침해사고 발생 시 나타난 공격유형과 유입되는 패킷속성에 따라 공격유형에 따라 패킷을 구현하였다. 또, 패킷사이즈 패킷생성의 구현을 위해 실제 침해사고가 발생하였던 샘플파일(pcap)의 통계량을 기초로 대량의 개체를 발생시키는 것을 모델

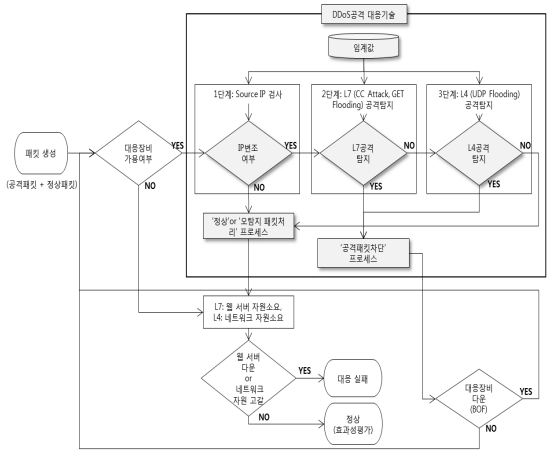

그림 5. DDoS공격 대응기술 효과성평가 순서도

링에 반영하였다. '정상'또는 '오탐지패킷 처리'프로세스는 일반 사용자가 정상적인 방법으로 서비스를 이용하고자하여 발생한 패킷과 탐지되지 못한 악의적인 공격패킷이 복합적으로 처리되는 프로세스이다. 이 패킷들은 대응기술의 자원을 소모하지 않고 L4, L7공격유형에 따라 네트워크 대역폭이나 웹서버 메모리의 용량(Capacity)을 소비한다. 반면에 공격이 탐지된 패킷들은 대응장비의 용량을 소비한 후 차단 처리되고, 한계용량이 초과될 때에는 시스템이 다운된다. 시뮬레이션 모델은 L4와 L7의 공격패킷은 현재까지 알려진 패턴을 기반으로 개체생성이 되었다는 가정이 존재한다.

3.4 효과성 평가

L4 UDP Flooding, L7 CC Attack/GET Flooding공격에 의해 수행된 시뮬레이션결과는 표 3과 같다. 시뮬레이션으로 측정된 가용도와 침입방어율은 특정 장비의 기술수준을 절대적인 수치로 보장하는 점수가 아닌 그림 5와 같이 구현된 대응기술 논리와 구현모델에 의한 상대점수를 의미한다. 표 3에서 L4대응기술이 임계치설정에 의한 탐지일 때 UDP Flooding의 공격에 대한 대응장비의 패킷차단율은 적어도 44.413%이상의 정확성을 보일 때 장비 가용도는 99.773%가 되고, 이때 DDoS공격에 대한 대응기술의 효과성은 75.117 [Tier 3]로 평가된다는 의미이다. 대응기술의 패킷차단율(탐지 정확도)이 높을수록 대응장비에 더 많은 부하를 주므로 대응장비의 가용도는 더 떨어질 수 있으나, 공격 대응(효과성평가)에 가능한 범위(종료 조건)내에 있으므로 가용도 등급이 더 높다하더라도 더 좋은 기술로 간주되진 않는다.

표 3. 시뮬레이션 결과 (단위: %)

대응 기술		공격유형 / 평가척도	L4 UDP Flooding	L7 CC / GET Flooding (Slowloris)	L4, 7 혼합공격 (50+50%)
L4	L7				
임계치	시그니쳐	패킷차단율	44.413	86.677	72.884
		정확도점수	55.587	13.323	27.116
		가용도	99.773	98.384	99.691
		가용도등급[3)]	Tier3	-	Tier1
		효과성평가	75.117	50.919	59.230
임계치 + 행동기반	시그니쳐	패킷차단율	57.882	86.677	80.884
		정확도점수	42.118	13.323	19.116
		가용도	99.996	98.384	99.738
		가용도등급	Tier4	-	Tier1
		효과성평가	67.700	50.919	54.750
임계치	행동기반	패킷차단율	44.413	90.884	96.33
		정확도점수	55.587	9.116	3.67
		가용도	99.773	100	99.711
		가용도등급	Tier3	Tier4	Tier1
		효과성평가	75.117	49.286	46.132
임계치 + 행동기반	행동기반	패킷차단율	57.882	90.884	99.999
		정확도점수	42.118	9.116	0.001
		가용도	99.996	100	99.760
		가용도등급	Tier4	Tier4	Tier2
		효과성평가	67.700	49.286	44.100

시뮬레이션 시간: 48시간, Warm-Up Time: 11분, 구현: In-Line, 시뮬레이션 반복 회수: 3회, 시뮬레이션 시간 단위: sec(초)
한계용량(Capacity): 4Gbps(1.25GB), 8G RAM(웹서버: 32G), 시스템/대응장비 다운 시간: 5분, 종료조건: 대응실패 3회 이상

이에 따른 L4 UDP Flooding 시뮬레이션 결과로 임계치 설정에 기반기술(75.117[Tier 3])이 임계치와 행동(통계)기반분석을 혼합한 기술(67.700[Tier 4])보다 더 효과적인 것으로 나타났다. 행동(통계)기반탐지가 공격패킷을 오탐지하는 경우가 많아 요구되는 최소한의 패킷차단율을 더 높게 요구하는 것으로 판단된다. L7 CC/GET Flooding시뮬레이션 결과에서는 시그니쳐기반 탐지기술(50.919[-])이 행동(통계)기반 탐지기술(49.286[Tier 4])보다 효과적인 것으로 나타났지만, 가용도가 떨어지므로 반드시'효과적이다'고 만은 할 수 없다. L4와 L7을 혼합한 시뮬레이션결과에서는 L4 대응기술의 차이에 따른 영향은 적었지만 L7 대응기술의 차이에 따른 결과 차이는 컸다. L7대응에서 시그니쳐기반 탐지기술의 경우 평가점수가 높게(59.230[Tier 1], 54.750[Tier 1]) 나타났지만 행동(통계)기반기술의 경우에는 시그니쳐기반 탐지기술과 비교하여 낮게(46.132[Tier 1], 44.100[Tier 2]) 계산되었다. 이는 표 1에서 탐지방식에 따른 침입탐지시스템의 특징을 설명하는 유사한 결과로 행동(통계)기반 분석기술이 시그니쳐기반 탐지기술이 보다 높은 오탐율을 보인다는 것을 증명한다.

3) 가용도 등급기준(Uptime Institute)[14]

기준	Tier 1	Tier 2	Tier 3	Tier 4
가용도	99.671%	99.749%	99.982%	99.995%

4. 결 론

본 논문에서는'DDoS공격'이라는 보안위협에 대해 '가용성'을 보안목표로 하는 대응기술의 효과성을 평가하는 방법을 제안해보았다. 보안통제영역과 성과지표의 가중치 산정을 위해 AHP분석을 이용한 정성적 평가와 기능점수의 계산을 위해 Arena시뮬레이션을 이용한 정량적 평가를 수행한다. AHP분석결과, 대응기술의 '정확성'을 대응장비의'신뢰성'보다 중요하게 생각하는 것으로 나타났다. L4, L7혼합공격 대응기술의 시뮬레이션결과로 L4의 임계치기반 대응기술과 L7의 시그니쳐기반 대응기술을 중복적용한 대응기술이 DDoS공격 대응에 가장 효과적인 것으로 나타났으나, 알려진 공격패턴으로 DDoS공격이 수행되었을 때에 가장 좋은 효과성을 갖는다는 결과이므로 한계점이 있다. 다시 말하면, 표 1에서 나타난 것과 같

이 행동(통계)기반탐지기술은 오탐율이 높으나 발견되지 않은 새로운 유형의 공격을 탐지할 수 있다는 것에 의미가 있다. 결론적으로 조직에 시그니쳐 업데이트 및 패턴 분석을 수행할 수 있는 충분한 운용인력이 존재하다면 임계치-행동기반 탐지기술의 중복사용이 가장 효과적이고, 그렇지 않다면 임계치-시그니쳐기반 탐지기술을 사용하는 것이 가장 효과적이다 할 수 있다.

효과성평가모형은 확장된 보안통제 및 관리 방법론으로써 앞서 연구된 기술적 관점에 국한되었던 DDoS대응 방안을 보다 다양하게 확장하여 설계할 수 있다. 즉, 보안목표를 두 가지이상의 복합적 요인으로 반영하는 것이 가능하다. 본 논문의 연구결과로 제안된 효과성평가모형은 새로운 보안위협에 대한 대응방안의 효과성을 검증하고 평가할 수 있는 방법으로써 활용될 수 있으리라 기대된다. 더욱이 보안제품이나 보안서비스가 논리적으로 표현이 가능하다면 Arena와 같은 범용시뮬레이터의 검증과정을 통해 보다 조직에 적합한 효과성평가가 가능하다.

참 고 문 헌

1. 김지연, 이주리, 박은지, 장은영, 김형종 (2009), "DDoS 공격 피해 규모 및 대응기법 비용분석을 위한 모델링 및 시뮬레이션 기술연구", *한국시뮬레이션학회 논문지*, Vol. 18, No. 4, pp. 39-47.
2. 김태원, 정재일, 이주영 (2010), "패킷 카운팅을 이용한 DoS / DDoS 공격 탐지 알고리즘 및 이를 이용한 시스템", *한국시뮬레이션학회 논문지*, Vol. 19, No. 4, pp151-159.
3. 이명수 등 (2010), *DDoS 공격 대응에 대한 한계용량 측정 방법론 연구*, 한국인터넷진흥원, KISA-RP-2010-0009, pp. 19, 150.
4. 이진수, 김두원, 박원형, 국광호 (2009), "네트워크 기반 DDoS 사이버 테러 분석 및 대응 방안 연구", *한국사이버테러정보진학회 정보·보안 논문지*, Vol. 9, No. 3, pp. 43-51.
5. 장범수, 이주영, 정재일 (2010), "False Alarm Rate 변화에 따른 DoS/DDoS 탐지 알고리즘의 성능 분석", *한국시뮬레이션학회 논문지*, Vol. 19, No. 4, pp. 139-149.
6. KrCERT/CC (2011), *인터넷 침해사고 동향 및 분석월호*, 한국인터넷진흥원, Vol. 12, pp. 50-51.
7. Andy Cuff, "Intrusion Detection Terminology (Part Two)", http://www.symantec.com/connect/articles/intrusion-detection-terminology-part-two, 2010.
8. Gary Locke, Patrick D. Gallagher (2010), *Recommended Security Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, Rev. 3, pp. 6-15.
9. Jie Wang, Raphael C.-W. Phan, John N. Whitley and David J. Parish (2011), "DDoS attacks traffic and Flash Crowds traffic simulation with a hardware test center platform", *Proc. of 2011 World Congress on Internet Security (WorldCIS)*, London, pp. 15-20.
10. Kevin Stine, Rich Kissel, William C. Barker, Jim Fahlsing, Jessica Gulick (2008), *Guide for Mapping Types of Information and Information Systems to Security Categories*, NIST Special Publication 800-60, Vol. 1, pp. 9-11.
11. Nidal Qwasmi, Fayyaz Ahmed, Ramiro Liscano (2011), "Simulation of DDoS Attacks on P2P Networks", *Proc. of 2011 IEEE 13th International Conference on High Performance Computing and Communications (HPCC)*, Oshawa, pp. 610-614.
12. QuEST Forum (2007), *TL 9000 Measurements Handbook*, Release 4.1, Appendix A, pp. 59-60.
13. Saaty, Thomas L. (2008), "Relative Measurement and its Generalization in Decision Making: Why Pairwise Comparisons are Central in Mathematics for the Measurement of Intangible Factors - The Analytic Hierarchy/Network Process", *Review of the Royal spanish Academy of Sciences, Series A, Mathematics (RACSAM)*, Vol. 102, No. 2, pp. 251–318.
14. W. Pitt Turner, John H. Seader, Vince Renaud, and Kenneth G. Brill (2008), *Tier Classifications Define site Infrastructure Performance*, The Uptime Institute, White Paper, pp. 15-17.

김 애 찬 (holytemple@korea.ac.kr)

2009 서울과학기술대학교 산업정보시스템공학과 학사
2009～2011 육군 정보체계·망관리장교
2012～현재 고려대학교 정보보호대학원 금융보안학과 석사과정

관심분야 : 금융보안, 컴퓨터시뮬레이션, 정보보호정책, 해킹·바이러스

이 동 훈 (donghlee@korea.ac.kr)

1983 고려대학교 경제학과 학사
1987 University of Oklahoma 전산학 석사
1992 University of Oklahoma 전산학 박사
1993～1997 고려대학교 전산학과 조교수
1997～2001 고려대학교 전산학과 부교수
2001～현재 고려대학교 정보보호대학원 교수, 부원장

관심분야 : 암호 프로토콜, 암호이론, USN이론, 키이론, 임베디드 보안

장 성 용 (syjang@seoultech.ac.kr)

1980 서울대학교 산업공학과 학사
1982 서울대학교 산업공학과 석사
1991 서울대학교 산업공학과 박사
1994～1995 University of Michigan 연구교수
1987～현재 서울과학기술대학교 글로벌융합산업공학과(산업정보시스템공학) 교수

관심분야 : 컴퓨터시뮬레이션, 제약경영, 프로젝트관리, E-business