디지털산업정보학회 논문지 제20권 제1호 - 2024년 3월
http://dx.doi.org/10.17662/ksdim.2024.20.1.109

관리자에게 경고 알림을 보낸 후 트래픽 측정을 기준으로 RDDoS 공격을 방어하는 시스템 설계

차 연 수* · 김 완 태**

Designing a system to defend against RDDoS attacks based on traffic measurement criteria after sending warning alerts to administrators

Cha Yeansoo · Kim Wantae

〈Abstract〉

Recently, a social issue has arisen involving RDDoS attacks following the sending of threatening emails to security administrators of companies and institutions. According to a report published by the Korea Internet & Security Agency and the Ministry of Science and ICT, survey results indicate that DDoS attacks are increasing. However, the top response in the survey highlighted the difficulty in countering DDoS attacks due to issues related to security personnel and costs. In responding to DDoS attacks, administrators typically detect anomalies through traffic monitoring, utilizing security equipment and programs to identify and block attacks. They also respond by employing DDoS mitigation solutions offered by external security firms. However, a challenge arises from the initial failure in early response to DDoS attacks, leading to frequent use of detection and mitigation measures. This issue, compounded by increased costs, poses a problem in effectively countering DDoS attacks.

In this paper, we propose a system that creates detection rules, periodically collects traffic using mail detection and IDS, notifies administrators when rules match, and Based on predefined threshold, we use IPS to block traffic or DDoS mitigation. In the absence of DDoS mitigation, the system sends urgent notifications to administrators and suggests that you apply for and use of a cyber shelter or DDoS mitigation. Based on this, the implementation showed that network traffic was reduced from 400 Mbps to 100 Mbps, enabling DDoS response. Additionally, due to the time and expense involved in modifying detection and blocking rules, it is anticipated that future research could address cost-saving through reduced usage of DDoS mitigation by utilizing artificial intelligence for rule creation and modification, or by generating rules in new ways.

Key Words : RDDoS, DRDoS, DNS Laundering DDoS, KISA of Cyber Shelter, DDoS mitigation, Alerts

* 서일대학교 정보통신공학과 학생(주저자)
** 서일대학교 정보통신공학과 조교수(교신저자)

Ⅰ. 서론

최근 민간기업 및 공공기관 보안 관리자에게 협박 메일을 보내고 DDoS(Distributed Denial of Service)를 수행하는 RDDoS(Ransum Distributed Denial of Service) 발생이 사회문제로 떠오르고 있다[1]. RDDoS는 기존에 나온 기술과 달리 남을 속이기 위한 기술과 시스템을 침투하기 위한 고급기술이 필요하지 않다는 장점이 있다. 클라우드플레어(Cloulplare)의 설문조사에서 응답자 10명 중의 1명은 RDDoS 공격 피해를 받았거나, 위협을 받았다고 응답했다[2]. 한국인터넷진흥원(Korea Internet & Security Agency, KISA)에서 발표한 2023년 상반기 사이버 위협 동향 보고서 결과에서 침해 유형별 신고 건수를 살펴보면 <표 1>과 같다.

〈표 1〉 침해 유형별 신고 건수

침해사고 종류	2022 (상반기)	2022 (하반기)	2023 (상반기)
DDoS 공격	48(10.1%)	74(11.1%)	124(18.7%)
서버 해킹	275(58.1%)	310(46.3%)	320(48.2%)
악성코드 (랜섬웨어 포함)	125(26.4%)	222(33.2%)	156(23.5%)
기타	25(5.3%)	63(9.4%)	64(9.6%)

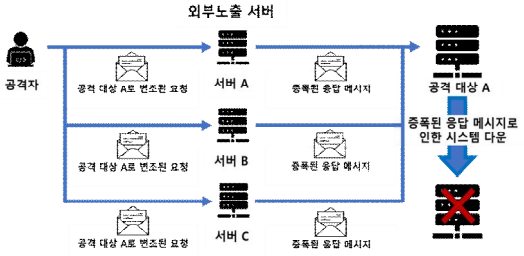
<표 1>에서 DDoS는 2023년 상반기 침해 유형별 신고 건수 중 18.7%로 사이버 위협 공격 중 3위이다. 그러나 2022년도 상반기 대비 2023년도 상반기에는 전년도 대비 8.6%의 DDoS 공격이 증가하는 것을 확인할 수 있으며, 신고 건수로는 약 2.5배가 증가한 것으로 확인된다[3]. 이처럼 DDoS 공격이 매년 증가하는데 비해 기업 및 기관의 보안담당자 대상으로 설문한 결과에서 전체 답변 중 23.8%의 응답자가 DDoS 공격에 대한 대응이 가장 어렵다고 응답했다. 이는 인력과 예산 문제로 볼 수 있으며, DDoS는 오랜 시간 동안 많은 인력이 트래픽(traffic) 탐지하고 공격 발생 시 DDoS 완화로 해결하는 과정에서 탐지와 완화에 높은 비용이 발생하기 때문이다. 완화는 초기 구축 비용과 많은 양의 데이터 사용이 필요하며, DDoS 공격 발생 시 제한된 데이터량의 초과로 인해 추가 요금이 발생하는 문제로 대응이 어렵다[4]. 따라서 본 논문에서는 탐지, 협박 메일 여부, 차단, 완화에 대하여 각 단계마다 관리자에게 알림을 전송하는 시스템을 제안한다. 탐지를 위한 도구는 와이어샤크(Whireshark)와 같은 IDS (Instrusion Detection System)로 탐지하며, 화이트 리스트(white list) 방식의 IPS(Instrusion Prevention System)를 사용하여 차단하고, 완화는 보안 및 클라우드 회사에서 제공하는 DDoS 완화 서비스, ISP(Internet Service Provider) 사업자의 블랙홀 라우팅(Black hole Routing), 한국인터넷진흥원의 사이버 대피소를 이용한다.

본 논문의 구성은 다음과 같다. 2장에서는 DDoS 공격 종류, 기존 DDoS 대응 방법에 관한 관련 기술에 대해 설명하고, 3장에서는 제안한 시스템에 대한 시스템 개요, 시스템 설계, 시스템 구현, 시스템 성능에 대해서 살펴본다. 4장에서는 결론을 기술한다.

Ⅱ. 관련 기술 동향

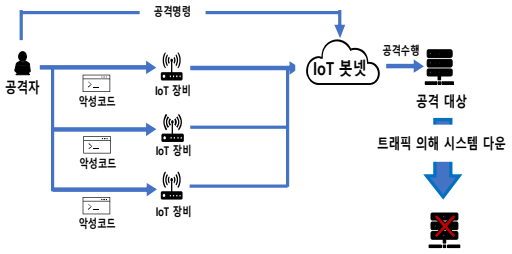
2.1 DDoS 공격 종류

DDoS 공격으로 크게 DDoS, DRDoS(Distributed Reflection DoS), RDDoS가 있다. DDoS는 공격자가 단말기에 악성코드를 감염된 다수의 좀비 PC를 이루는 봇넷(Bot-Net)에 공격 명령을 내려 공격 대상 시스템이 대규모 트래픽을 발생하는 공격을 말한다.

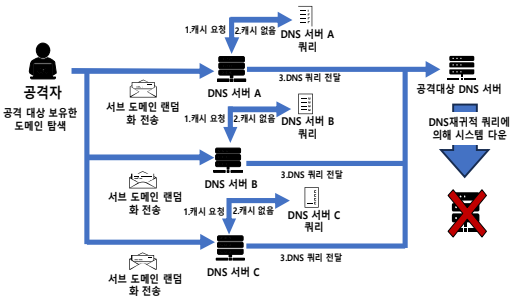


〈그림 1〉 DRDoS 공격과정

DRDoS는 <그림 1>과 같이 공격 대상의 IP주소로 변조하여 외부에 노출된 서버에 요청하고 외부에 노출된 서버는 공격 대상 IP주소를 증폭하여 패킷 전송을 통해 공격 대상에게 대규모 응답 메시지가 발생하게 유도하여 시스템이 장애가 발생하도록 하는 방식이다. DRDoS는 다수의 좀비 PC 없이 공격 대상에게 대규모 트래픽을 발생시키고, 실제 공격이 공격자와 무관한 외부의 노출된 서버를 통해 수행함으로써 공격자의 위치가 노출되지 않는 장점이 있다. 대표적인 공격으로는 NTP (Network Time Protocol) 증폭 공격, 멤케시드(Memcashed) 공격, DNS(Domain Name System) 증폭 공격 등이 있다[5]. IoT(Internet of Things)를 이용한 DDoS 공격은 <그림 2>처럼 공격자가 IoT 장비를 악성코드로 감염시킨 후에 IoT 봇넷 네트워크를 구성하여 공격 대상에게 DDoS를 수행하는 방식이다. IoT 장치는 저전력 동작으로 가벼운 프로그램을 사용하여 상대적으로 무거운 보안프로그램을 설치할 수 없으므로 보안에 약하다는 단점이 있으며 공격자는 주로 봇넷을 이용하여 공격한다[6].

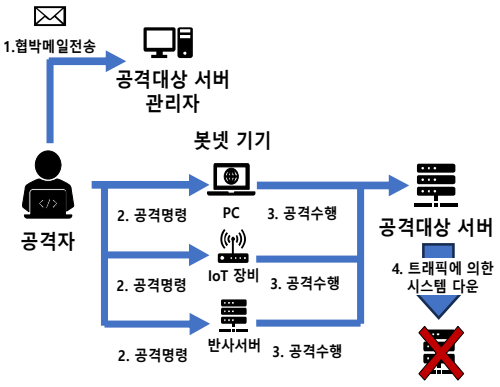


〈그림 2〉 IoT 봇넷을 이용한 DDoS 과정



〈그림 3〉 DNS 세탁 공격과정

DNS 세탁 공격(DNS Laundering DDoS)은 경제용어인 자금세탁에서 비유해서 나온 말로, 저명하거나 신뢰가 있는 DNS를 이용하여 불법적 트래픽을 정상적인 트래픽인 것처럼 위장하여 DDoS를 수행하는 방식이다. <그림 3>과 같이 공격자가 공격 대상이 관리하는 도메인에 대한 서브 도메인을 랜덤화하여 쿼리를 요청하는 방식이다. 재귀적 DNS는 랜덤한 서브 도메인을 찾지 못해 해당 도메인을 관리하는 DNS 서버에 쿼리를 전송하고, 공격 대상 서버는 정상적으로 쿼리를 실행할 수 없을 정도의 대규모 쿼리를 요청을 받게 된다. DNS 세탁 공격은 구글 DNS IP주소와 같이 ISP 사업자의 IP주소와 같은 신뢰성 있는 DNS 주소를 이용하여 공격하기 때문에 정상적 쿼리와 악의적 쿼리를 분류하여 차단하기 어려운 것이 특징이다[7].



〈그림 4〉 RDDoS 공격과정

RDDoS는 기업 또는 기관을 대상으로 협박 메일을 전송하여 금전을 요구하는 방식에 따라 DDoS를 수행하는 공격을 말한다. RDDoS는 공격 대상이 관리하는 네트워크 전체 또는 일부를 대상으로 DDoS 공격을 실행한 다음에 피해자에게 공격을 중단하고 싶으면 금전을 요구하거나, DDoS 수행 전에 금전을 요구한 다음에 금전을 지불하지 않으면 DDoS를 수행하는 것을 말한다. RDDoS 공격과정은 <그림 4>와 같이 공격자가 관리자에게 협박 메일을 전송한다. 협박 메일을 전송하여 자신이 제어하는 봇넷 기기들에게 공격을 명령하여 IoT 장비, 반사 서버, 좀비 PC를 통해 생성된 대규모 트래픽을 공격 대상 서버에 발생시켜 시스템 장애를 발생한다. RDDoS 협박 메일은 일반 메일처럼 상대방을 속이는 기술과 해당 시스템에 침투하기 위한 고급 기술이 필요하지 않고, 랜섬웨어와 달리 전문적인 지식도 필요하지 않아 단순히 DDoS를 실행만 하면 된다는 특징을 가지고 있다. 추가로 DDoS 공격뿐만 아니라 협박 메일 속에 악성코드를 담겨있는 링크를 클릭하게 유도하여 데이터의 일부 및 전부를 암호화 및 유출 등 2차 협박으로 복합적으로 활용하는 경우가 있다. 기존에 DDoS 공격과 알려지지 않은 DDoS 공격방식과의 결합을 통해 더욱 정교해지고 세밀한 공격이 가능하며 최근에는 시스템의 성능을 최대한으로 사용하여 시스템 자원과 대역폭을 마음대로 설정할 수 있는 가상화 기술을 사용하여 구축한 가상 봇넷을 이용한 DDoS와 결합한 RDDoS는 다양한 공격방식이 증가가 예상되고 있다.

2.2 기존 DDoS 대응 방법

DDoS의 대응 방법으로는 IDS/IPS를 사용한 탐지와 차단 또는 WAF(Web Application Firewall), DDoS 완화, 블랙홀 라우팅, 사이버 대피소 이용이 있다. 방화벽 장비 또는 소프트웨어는 기본적으로 규칙을 작성하여 규칙에 따라 특정 포트 및 IP주소에 대한 허가 또는 블록 처리를 수행한다. 하지만 일반적으로 방화벽은 OSI 3계층에서 4계층까지만 작동하는 단점이 있기 때문에 3계층부터 7계층에서의 탐지와 차단은 IDS와 IPS를 사용한다.

IDS는 네트워크 트래픽의 이상을 탐지하고 분석하는 N-IDS(Network-IDS)와 시스템 이상을 탐지 및 분석하는 H-IDS(Host-IDS)로 구분한다[8]. IPS는 주로 인라인 방식으로 설치하여 모든 트래픽이 IPS를 통해 전달하도록 구성하여 실시간 패킷을 차단하는 장비 및 프로그램이다[9]. IDS와 IPS는 오용 방식 또는 이상 방식을 사용하는데 오용방식은 기존에 알려진 공격방식 및 패턴을 입력하여 규칙을 만들어 탐지하고 차단하는 방식이다. 알려진 공격 방식인 경우 대부분 탐지와 차단이 가능하지만 알려지지 않는 공격은 탐지 및 차단이 어렵다는 단점이 있다. 이상 방식은 정상적으로 사용한 방식이나 패턴을 저장하고 분석해 기준을 설정하여 탐지 및 차단하는 방식이다. 이 방식은 알려지지 않는 공격에 대응하는 장점을 가지며 저장된 정상 사용자의 행위 패턴 오류를 공격으로 오인하여 대응 및 정상 사용자를 이용한 공격방식을 사용하는 경우 대응하지 못한다는 단점이 있다.

WAF는 OSI 4계층에서 7계층까지 동작하는 IDS/IPS 달리 OSI 7계층인 애플리케이션 층에서 분석하고 작동하는 방화벽으로 주로 애플리케이션 서버와 인터넷 사이에 설치하여 대응한다. IDS/IPS가 검사영역이 더 광범위이지만 웹 중심적으로 정밀검사하고 방어하기 때문에 SQL 인젝션(Structured Query Language Injection), XSS(Cross Site Scripting), CSRF(Cross Site Request Forgery) 공격을 식별하고 대응하기 때문에 웹 영역에서는 IDS/IPS보다 WAF이 성능이 뛰어나다. 기본적으로 규칙 기반 WAF과 이상 방식 WAF로 구분한다. 규칙 기반은 사전에 비정상 행위에 대하여 규칙 및 서명을 생성하여 악의적 트래픽과 정상적 트래픽을 구분하여 대응하는 방식이다. 알려진 위협에서는 성능에 뛰어나게 작동하지만 사용자 동작 패턴 및 민감한 데이터, 애플리케이션 데이터 등을 고려하는 능력이 부족해서 정상 트래픽과 악의적 트래픽을 정확하게 구별하기 어렵고 새로운

공격이나 제로데이 공격에 대한 대응이 어렵다. 새로운 공격에 대응하기 위한 규칙을 추가 및 수정하거나 잘못 설정한 경우 대응하지 못하는 단점이 있다. 이상 기반 방식은 정상적 동작의 규칙과 패턴을 학습하여 저장하고 저장된 패턴과 다른 패턴을 동작하는 트래픽을 대응하는 방식이다. 제로데이 공격과 새로운 공격방식에 대한 대응이 가능하고 사용자 동작 패턴, 민감한 데이터, 세션 데이터 등 애플리케이션 데이터를 분석이 가능하다는 특징을 가진다. 그러나 잘못된 학습을 통해 합법적 트래픽을 공격으로 인식하거나 정상 트래픽의 패턴 방식들이 많은 용량의 데이터 필요로 하고 사용하여 공격에 대응하지 못하는 단점이 있다[10].

DDoS 완화는 DDoS 공격으로부터 서버 및 시스템을 보호하기 위해 공격에 저항하여 공격 피해를 최소화하기 위한 기술을 말한다[11], DDoS 완화는 물리적으로 장비를 통해 시스템을 구축하거나 클라우드를 통한 외부 DDoS 완화를 사용한다. 장비를 통한 구축으로는 서버 용량을 대규모로 구축하고 분산처리하며, 로드 밸런스 시스템을 추가로 구축하는 방식이 있지만 초기의 구축비용과 보안 인력이 많이 필요하고 DDoS 공격이 대규모로 이루어지지 않는 경우 예산이 낭비되는 단점이 있다. 클라우드를 통한 DDoS 완화는 외부 기업이나 기관의 솔루션을 통해 탐지, 차단, 분석제공을 클라우드 형태로 제공받는 형식이며[12], 일반적으로 초기에 구축비용이 없지만 설정된 데이터 사용량이 초과하면 데이터 초과요금이 발생하며, 클라우드 서비스 구독이 없는 경우에는 클라우드 구축비용 및 다른 클라우드 서비스 구독 비용 신청을 통해 추가적으로 비용이 발생하는 단점이 있다[13]. 이처럼 DDoS 완화는 사용이 편리하다는 장점이 있지만 클라우드의 구독비용과 데이터 초과 비용이 발생하는 단점이 있어 비용 측면에서 DDoS 완화를 사용하기가 부담스럽기 때문에 DDoS 완화 대신 블랙홀 라우팅이라는 ISP 사업자가 제공하는 서비스를 사용한다. 블랙홀 라우팅은 라우터에 BGP(Border Gateway Protocol)를 활용하여 BGF 라우팅 테이블에 특정 IP주소를 포워딩하도록 설정하며, 해당 IP주소의 라우터는 모든 패킷을 NULL로 지정하여 모든 패킷을 삭제(Drop)한다[14]. 그러나 정상 사용자와 악의적 사용자와 동시에 존재하는 트래픽에서 블랙홀 라우팅을 설정하면 모두 차단하여 정상 사용자가 서비스를 이용하지 못하게 된다.

한국 인터넷 진흥원에서는 중소기업 대상으로 무료로 제공하는 사이버 대피소를 제공하고 있으며, 사이버 대피소는 공격 대상의 IP주소를 사이버 대피소의 IP주소로 변경한 후 공격 트래픽을 사이버 대피소에 전송하여 방어하는 방식이다. 사이버 대피소는 3단계로 구성하며 1단계는 ISP 사업자와 협업을 통해 단순한 네트워크 자원을 소모하는 DDoS 공격을 차단한다. 2 단계는 QoS(Quality of Service) 장비를 사용하여 발신 IP주소 분석을 통해 정상 사용자와 좀비 PC를 구분한다. 3 단계는 L7 스위치와 웹 캐싱, WAP 장비 등을 사용하여 트래픽 단순화를 통해 서버를 분산하여 서버의 가용성을 확보 한다 [15]. 하지만 한 달 동안 보호하고 위협이 있을 경우 3개월까지만 보호할 수 때문에 주기적으로 신청해야하며, 주기적인 시스템이 보호 여부를 확인해야 하는 단점을 가지고 있다[16].

Ⅲ. 제안하는 시스템

3.1 시스템 개요

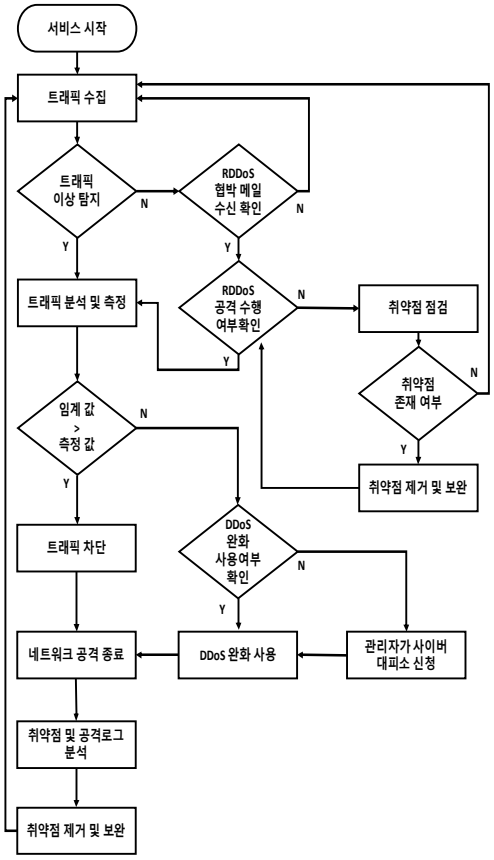
DDoS 공격이 증가하는 추세로 인해 DDoS공격이 RDDoS, DRDoS, DNS 세탁 공격 등 다양한 DDoS가 파생되어 공격에 다양성이 추가되었다. 스칸디나비아의 사례[17]를 보면 초기 몸값 요구가 3,500달러에서 3백만 달러로 증가하는 것을 볼 수 있는데 초기 몸값 요구에 비례하여 점점 증가하고 있다. 이를 통해 몸값 요구를 들어주는 것은 최선의 대응이 아닌 것으로 볼 수 있다. 따라서 RDDoS를 대응하는 시스템과 기존에 알려진 DDoS와

새로운 DDoS 공격에 대응하여 피해를 최소화하는 시스템 설계가 필요하다. 따라서 RDDoS를 대응하기 위해서 실시간으로 트래픽 측정과 메일을 탐지하며 특정 패턴이나 규칙을 설정하여 규칙에 맞으면 관리자에게 알림을 보낸다. 트래픽 규칙에 기준을 임의로 설정하여 기준을 초과하면 특정 파일을 생성시킨다. 특정 파일이 존재하면 임계값 초과로 DDoS 완화를 사용하고 존재하지 않으면 트래픽을 차단하는 방식이다. DDoS 완화가 없을 경우 관리자에게 긴급알림을 보내 DDoS 완화 및 사이버 대피소를 신청하여 대응하는 시스템을 제안한다.

3.2 시스템 설계

<그림 5>는 알람을 통해 RDDoS 대응하는 시스템이다. 트래픽 수집 방법으로 와이어샤크, 스노트(SNort), IDS 등을 사용한다. 트래픽 탐지규칙은 PPS(Packet Per second), BPS(Bit per Second), IP(Internet Protocol)주소, 연결시간, 최저 전송속도, 최대 연결 속도, 동시 접속자 수, 접속자 수, 웹 콘텐츠 속도 등 규칙을 만들고 규칙의 위반한 경우를 탐지하고 mpstat, iftop. vmstat등 분석 프로그램을 이용하여 트래픽을 측정한다[18]. 측정된 값과 임계값을 비교하여 임계값이 측정값보다 작은 경우 패킷을 차단한다. 차단은 들어오는 특정 포트 차단 및 연결시간 횟수 초과, 특정 IP 차단 등 규칙이 설정된 방화벽 또는 IPS를 사용한다. 측정값이 임계값 보다 큰 경우는 DDoS 완화를 사용하고 알람을 보낸다. DDoS 완화 사용이 불가능한 경우 관리자에게 긴급알림을 보내고 관리자는 긴급알림을 확인하여, KISA에 제공하는 사이버 대피소 및 IPS 사업자의 블랙홀 라우팅을 긴급으로 신청하여 사용한다. 트랙픽 측정값이 정상인 경우는 DDoS 종료로 관리자에게 알림을 보낸다. 관리자는 알림 코드를 확인하면 시스템 로그와 DDoS 완화 로그 등을 바탕으로 취약점을 분석하고 보완한다.

취약점 분석으로는 알치니(Arachni), 말테고(Maltego), 백트랙(BackTrack)등을 이용하여 취약점 분석과 공격 로그, DDoS 완화 로그 등 통해 취약할 부분 제거 및 시스템 자원 증가, 트래픽 차단 규칙 추가, 보안 솔루션 구매 등을 통해 시스템을 보완하여 트래픽 수집에 들어간다. 또한 트래픽에 이상이 없는 경우는 RDDoS, DDoS, Attack 등의 내용을 가진 협박 메일을 확인하여 알림을 보내고 공격 수행 여부를 확인한다. 이때 메일 수신이 확인되지 않으면 다시 트래픽 수집을 진행한다. 공격 수행 여부가 확인되지 않으면 취약점 점검을 진행하여 취약점이 발견되면 제거하고 아닌 경우 다시 공격 수행 여부를 확인한다. 공격 수행 여부가 확인되면 제안한 DDoS 대응 방식으로 진행한다.



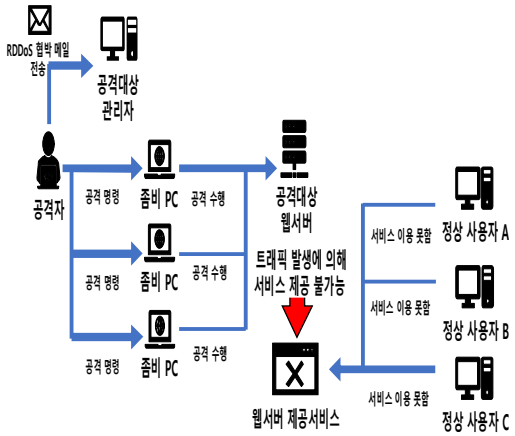
〈그림 5〉 알림을 통해 RDDoS 대응하는 시스템 흐름도

3.3 시스템 구현

〈표 2〉 시스템 설정 정보

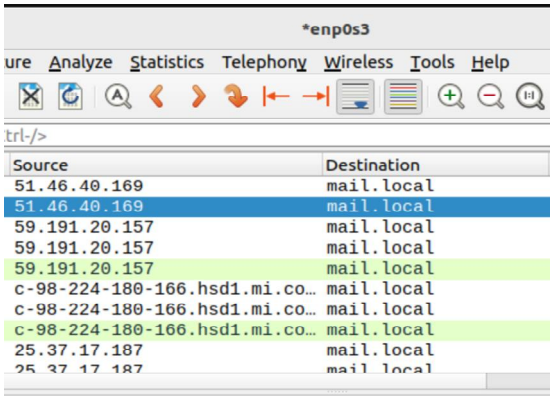
서버이름	운영체제	도메인	IP주소
kari	Kari Linux	없음	192.168.182.212
red	Ubuntu	mail.com	192.168.182.63

본 논문에서 제안하는 시스템 구현을 위한 설정 정보는 <표 2>와 같다. kari는 칼리 리눅스 운영체제를 사용하였고, DDoS 공격 서버로 설정했다. red는 Ubuntu 운영체제와 도메인 이름이 mail.com을 설정했다.



〈그림 6〉 Kari 공격과정

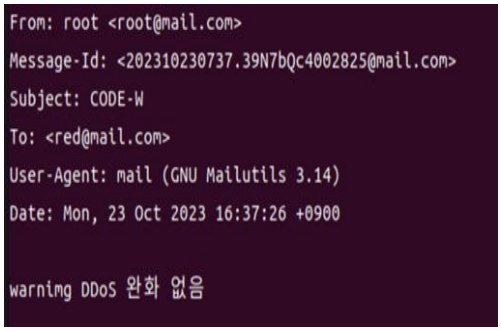
<그림 6>는 Kari가 수행한 공격 절차이다. 관리자에게 협박 메일을 보낸 후 좀비 PC를 통해 red 서버 대상으로 공격해서 서비스 거부 상태를 만들어 정상 사용자들이 red의 웹서비스를 제공하지 못하게 구성한다. 실제 Kari에서 Hping3 프로그램을 사용하여 red에게 TCP-flooding 공격을 수행하고 자신의 IP주소를 스푸핑하여 대규모 공격 대상인 red를 향해 DDoS를 수행한다[19]. <그림 7>은 red에서 대량의 TCP 연결 요청을 와이어샤크를 통해서 탐지한 결과이며, <그림 8>은 RDDoS 협박 메일과 IDS를 이용하여 kari 에서 수행한 DDoS 공격 탐지한 후 트래픽을 측정하여 설정된 임계값을 초과해 DDoS 완화를 사용한 것을 red 사용자에게 알림을 보낸 후 mail 명령어를 통해 확인한 결과이다.



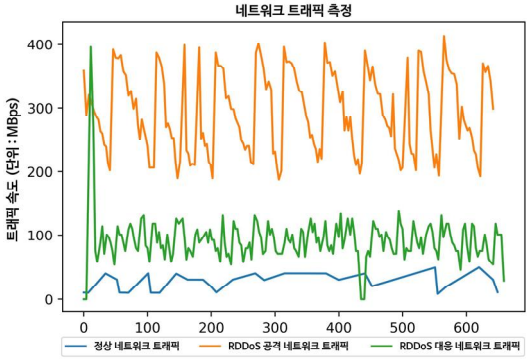
〈그림 7〉 와이어샤크를 사용하여 탐지된 공격 패킷

<그림 9>는 <그림 8>과 달리 DDoS 완화 없이 관리자에게 긴급알림을 보낸 것을 확인한 결과이다. 관리자는 <그림 8>을 확인하면, 설정한 방법으로 사이버 대피소 또는 DDoS 완화 솔루션을 사용하도록 설정하고, 다음 공격 종료 후 서버의 취약점을 점검한 후 공격 로그, DDoS 완화 로그, 시스템 로그 등 다양한 로그를 바탕으로 시스템을 분석하여 다음 공격에 대비하여 네트워크 트래픽용량 증가, IDS/IPS 탐지 및 차단 규칙의 수정 및 추가 등의 시스템을 보완한다.

〈그림 8〉 리눅스 명령어 알림 메일 확인



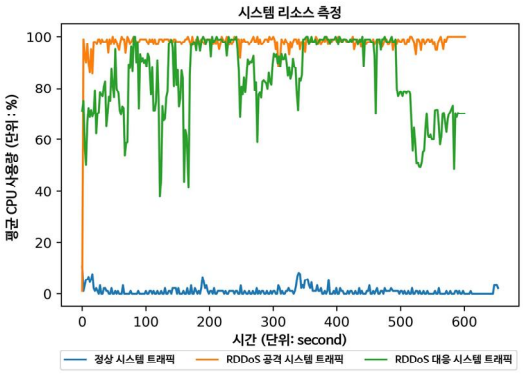
〈그림 9〉 DDoS 완화가 없어 수신된 긴급알림



〈그림 10〉 시스템 상태별 네트워크 트래픽 속도 측정

3.4 시스템 성능

<그림 10>은 시뮬레이션을 통해 측정한 네트워크 트래픽 결과를 나타낸 그래프이다. 가로축은 시간이고 세로축은 네트워크 속도를 의미한다. 각각 정상 네트워크 트래픽, RDDoS 공격 네트워크 트래픽, RDDoS 대응 네트워크 트래픽으로 1초당 발생하는 네트워크 속도를 측정했다. 공격이 발생한 경우 네트워크 트래픽 속도가 400Mbps로 증가한 것을 확인할 수 있다. 트래픽과 임계값 비교를 통해 DDoS 완화 및 트래픽 차단을 사용하여 평균적으로 네트워크 속도가 약 100Mbps로 줄어든 것을 확인했다. <그림 11>은 시스템 리소스를 측정한 결과를 나타낸 그래프이다. 가로축은 시간이고 세로축은 CPU 평균 사용량을 의미한다. 각각 정상 시스템 트래픽. RDDoS 공격 시스템 트래픽, RDDoS 공격 대응 시스템 트래픽으로 1초당 사용되는 CPU 사용량을 측정했다. 공격이 발생한 경우 CPU 평균 사용량이 100%로 증가한 것을 확인할 수 있다. 이를 통해서 임계값과 비교하여 트래픽 차단 및 DDoS 완화를 사용하여 CPU 평균 사용량이 줄어진 것을 확인할 수 있다.



〈그림 11〉 시스템 상태별 시스템 사용량 측정

Ⅳ. 결론

본 논문에서는 탐지, 메일 수신여부, 임계값 측정, 차단, 완화에 대해 관리자에게 알림을 보내 RDDoS를 대응하는 시스템을 제안했다. RDDoS 정의, DDoS의 공격추세, 보안관리자의 DDoS 대응 상황을 조사하여 RDDoS의 대응 시스템이 필요성을 제시하였으며, DDoS 공격 종류, 기존 대응 방법, 제안한 시스템 흐름도, 시스템 구현에 대하여 설명하였다. DDoS 공격 종류로는 DDoS와 DRDoS, IoT 봇넷을 이용한 DDoS, DNS 세탁 공격, RDDoS의 공격 원리 및 장단점을 설명하였다. RDDoS가

기존에 알려진 DDoS 공격과 알려지지 않는 공격을 결합한 공격 수행이 가능하고 시스템 침투 및 남을 속이기 위한 고급 기술이 필요하지 않는 장점이 있어 RDDoS 공격추세가 증가할 것으로 예상됨에 따라, 기존 대응 방법은 탐지와 차단, WAF, DDoS 완화, 블랙홀 라우팅, 사이버 대피소에 대한 설명과 IDS와 IPS로 탐지와 차단하는 방법인 오용방식과 이상방식의 문제점을 분석하였다. 제안한 시스템 흐름도를 통해 트래픽 수집 중 이상 발견을 통해 임계값을 설정하여 측정값이 임계값 보다 작으면 트래픽 차단하고 초과한 경우 DDoS 완화를 통해 대응하는 시스템을 설계하였으며, 트래픽 수집의 이상이 없는 경우 관리자의 메일을 확인하여 RDDoS 협박메일 수신하면 공격 수행 여부를 판단하여 공격 수행 전이면 취약점을 점검하여 제거하고 수행 중이면 기존 DDoS공격 대응하는 시스템을 설계하였다. 설계한 시스템을 통한 시뮬레이션으로 트래픽 이상, RDDoS 협박 메일을 확인하여 트랙픽 측정을 통한 임계값에 따라 IPS로 차단 및 DDoS 완화를 사용하였으며, 추가로 DDoS 완화가 없는 경우 관리자에게 긴급알림을 보내는 시스템을 설계하여 <그림 9>와 같은 알림을 보내 관리자 DDoS 완화를 신청 및 사이버 대피소를 사용하게 했다.

본 논문에서 제안한 시스템 시뮬레이션 결과 알림을 통해 RDDoS 공격을 초기에 발견하고, RDDoS의 공격에 대응할 수 있는 것을 확인하였다. 화이트 리스트 방식으로 기존에 알려진 공격을 차단했으며 리소스 부족 및 기존에 알려지지 않는 공격방식에 의해 차단이 불가능한 경우에는 DDoS 완화를 사용하여 대응할 수 있다. 이러한 과정을 통해 기존에 알려진 공격과 새로운 방식의 DDoS 대응을 통해 DDoS 공격이 감소하는 것을 확인할 수 있었다. 또한 임계값을 잘못 설정한 경우 시스템이 정상적으로 처리하는 대신에 DDoS 완화를 사용하여 DDoS 완화 비용과 공격 종료 후 시스템 분석과 로그를 바탕으로 트래픽 및 메일 탐지 및 차단규칙 업데이트에 시간과 비용이 증가하는 문제가 있을 것으로 추정한다. 따라서 시스템 취약점 분석 정리, 탐지와 차단규칙의 수정 및 관리를 인공지능으로 학습하여 적용하면 관리자의 DDoS 대응관리 비용이 감소해질 것으로 예상된다. 추가로 DDoS 완화 사용 후 시스템을 보완할 때 특정 IP 대역과 접속자의 임계값을 무시하는 등의 시스템에 알맞은 규칙을 생성하면 DDoS 완화의 사용횟수를 줄임으로써 최종적으로 비용이 감소해질 것으로 보인다.

참고문헌

[1] 문기운・이종혁," 최신 랜섬웨어 동향 및 발전 방향," 정보보호학회지, 제32권, 제3호, 2022, pp.33-39.

[2] Yoachimik, O. and Pacheco, J., "DDoS threat report for 2023 Q2", CLOUDFLARE, https://blog.cloudflare.com/ddos-threat-report-2023-q2, 2023.07.18.

[3] 한국인터넷진흥원 , “ 2023년 상반기 사이버 위협 동향 보고서,” https://www.kisa.or.kr/20205/form?postSeq=1024&lang_type=KO#fndoDocumentPreview, 2023.08.22.

[4] 김경애, “ [2023 디도스 대응 리포트] 디도스 융단폭격에 기업·기관 ‘휘청’,” 보안뉴스, https://m.boannews.com/html/detail.html?idx=115528, 2023.04.01.

[5] 백남균, “DRDoS 공격에 대한 다단계 탐지 기법,” 한국정보통신학회 논문지, 제24권, 제12호, 2020, pp.1670-1675.

[6] Al-Duwairi, B. et al., “SIEM-based detection and mitigation of IoT-botnet DDoS attacks,” International Journal of Electrical and Computer Engineering, Vol. 10, No.2, 2020, pp.2181-2191.

[7] 김선애, “신뢰 악용하는 ‘DNS 세탁 디도스’ 유행,” 데이터넷, https://www.datanet.co.kr/news/articleView.html?idxno=185472, 2023.07.20.

[8] Ashoor, A.S., and Gore, S., “Importance of Intrusion Detection System (IDS),” International

Journal of Scientific & Engineering Research, 2011, Vol. 2, No 1.

[9] 전용희, “침입방지시스템(IPS)의 기술 분석 및 성능평가 방안,” 정보보호학회지, 제15권, 제2호, 2005, pp.63-73.

[10] Harish Kumar, J. and Godwin Ponsam, J., Securing Web Application using Web Application Firewall (WAF) and Machine Learning," First International Conference on Advances in Electrical, Electronics and Computational Intelligence, 2023, pp.1-8.

[11] Wikipedia, “DDoS mitigation,” https://en.wikipedia.org/wiki/DDoS_mitigation#cite_note-1, 2024.01.03.

[12] Osanaiye, O. et al., “Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework,” Journal of Network and Computer Applications. Vol.67, 2016, pp. 147-165.

[13] AWS, “ AWS Shield 요금,” https://aws.amazon.com/ko/shield/pricing

[14] 김태원・정재일・이주영, “패킷 카운팅을 이용한 DoS/DDoS 공격 탐지 알고리즘 및 이를 이용한 시스템,” 한국시뮬레이션학회 논문지, 제19권, 제4호, 2010, pp.151-159.

[15] 최지우・천명진・홍도원, “DNS을 목표한 DDoS공격에 효과적인 대응 방법 제안,” 한국정보보호학회, 제23권, 제4호, 2013, pp.729-735.

[16] 한국인터넷진흥원, “DDoS 공격대응,” https://www.kisa.or.kr/1020202, 2022.02.08.

[17] Stefanie Schappert, “SAS faces new $3m ransom demand to halt ongoing attack,” cybernews, https://cybernews.com/security/sas-3m-ransom-demand-anonymous-sudan-ongoing-attack, 2023.05.31.

[18] 노츠코의 주경야독, “6.1: CPU, 메모리, 네트웍 및 디스크 (I/O 작업) 관련 통계치 확인하기,” https://nochoco-lee.tistory.com/356, 2020.07.02.

[19] 지니온, “ Kali Linux의 hping3를 이용한 Port Scanning, DoS 공격,” https://blog.naver.com/zinion_blog/222110291922, 2020.10.08.

■ 저자소개 ■

차 연 수
(Cha Yeansoo)

2024년 2월
서일대학교 정보통신공학과
(공학사)

관심분야 : 정보보안, 네트워크 시스템 보안, 네트워크 방화벽 및 해킹방지
E-mail : kszm3434@gmail.com

김 완 태
(Kim Wantae)

2011년 3월~현재
서일대학교 정보통신공학과 조교수
2011년 2월 한국항공대학교 정보통신공학
(공학박사)
2004년 2월 한국항공대학교 정보통신공학
(공학석사)

관심분야 : 네트워크 시스템 보안, 통신시스템 설계, 모바일 응용 S/W, AI Smart Car
E-mail : wtkim@seoil.ac.kr

논문접수일 : 2024년 1월 23일
수정접수일 : 2024년 2월 26일
게재확정일 : 2024년 3월 02일