http://dx.doi.org/10.14400/JDC.2015.13.10.279

웹 기반 실시간 DNS 질의 분석 시스템

장상동
경남대학교 컴퓨터공학과

A RealTime DNS Query Analysis System based On the Web

Sang-Dong Jang
Dept of Computer Secience and Engineering, Kyungnam University

요 약 본 논문은 DNS를 이용한 보안 위협에 대응하기 위한 웹 기반의 실시간 질의 분석 및 제어 시스템을 제안한다. 제안 시스템은 DMZ로 유입되는 DNS 질의를 미러링하여 데이터를 수집하고 분석한다. 그 결과로 DNS 보안 위협을 발견하면 방화벽 필터링 정보로 사용하며 DNS 질의의 통계정보를 실시간으로 웹 서비스한다. DNS특정 문제만을 해결하기 위한 기존의 시스템에 비해 제안 시스템은 DNS 스푸핑, DNS 플러딩 공격, DNS 증폭 공격 등 다양한 공격에 대응하며, 불법적인 DNS의 사용을 미리 차단함으로써 내부로부터 발생할 수 있는 불법적인 침해 사고를 예방한다. 웹으로 실시간 DNS 통계 정보를 제공하고 GeoIP를 이용한 위치정보와 Google API의 지도를 이용하여 DNS 질의 발생과 관련하여 위치 정보를 제공한다. 현재까지의 DNS 공격에 대한 경험과 지식이 부족하기 때문에 웹 서비스와의 보안 융합 시스템을 이용하여 구축한 데이터베이스는 DNS 관련 보안 침해 공격에 대한 연구에 있어 향후 중요한 자료로 사용될 수 있다.

주제어 : Realtime Web Service, DNS Flooding Attack, DNS Amplification Attack, DNS Spoofing, 보안 융합

Abstract In this paper, we present the design and implementation of a realtime DNS Query Analysis System to detect and to protect from DNS attacks. The proposed system uses mirroring to collect data in DMZ, then analizes the collected data. As a result of the analysis, if the proposed system finds attack information, the information is used as a filtering information of firewall. statistic of the collected data is viewed as a realtime monitoring information on the web. To verify the effictiveness of the proposed system, we have built the proposed system and conducted some experiments. As the result, Our proposed system can be used effectively to defend DNS spoofing, DNS flooding attack, DNS amplification attack, can prevent interior network's attackers from attacking and provides realtime DNS query statistic information and geographic information for monitoring DNS query using GeoIP API and Google API. It can be useful information for ICT convergence and the future work.

Key Words : Realtime Web Service, DNS Flooding Attack, DNS Amplification Attack, DNS Spoofing, Security Convergence

Received 10 August 2015, Revised 15 September 2015
Accepted 20 October 2015
Corresponding Author: SangDong Jang (Dept of Computer Secience and Engineering, Kyungnam University)
Email: angong@kyungnam.ac.kr

ISSN: 1738-1916

1. 서론

최근 DNS를 목표로 하는 침해사고는 정부기관이나 금융기관을 비롯하여 인터넷 사이트를 마비시키는 등 인터넷 보안을 위협하고 있다. 보안을 위협하는 공격 형태가 과거 단순한 자기 과시나 만족을 위해 자행되던 무차별적인 공격과는 다르게 세분화, 조직화되고 있기 때문에 DNS 역시 보안성 향상을 위해 취약점과 위협에 대응하는 다양한 연구와 솔루션이 필요하다.

인터넷 서비스와 밀접한 관계를 갖는 DNS 장비에 장애가 발생할 경우 기존의 보안장비가 무력화될 가능성이 높다. DNS에 문제가 발생할 경우 DNS 서비스뿐만이 아니라 해당 DNS를 사용하는 모든 응용프로그램 사용까지도 문제가 발생하기 때문에 즉, DNS 서비스의 장애가 곧 인터넷의 장애로 이어지기 때문에 DNS 시설 장비의 방어는 매우 중요하다[1]. 특히 ITC 융합으로 더욱 많은 곳에서 DNS를 필요로하며, 정부는 사이버위협에 선제 대응하기 위해 융합보안 시범 사업을 실시할 계획이다[2].

본 논문에서는 DNS의 취약점을 개선하고 최소화하여 DNS 스푸핑에 대처하고, 대규모 DDoS 공격에 대응하여 보안성을 향상시킬 수 있도록 실시간 DNS 질의/응답 모니터링하고 제어하는 시스템을 제안한다.

본 논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에서는 DNS 특징과 다양한 DNS를 이용한 침해 공격 기법과 방어 기법에 그리고 제안 시스템 구현에 사용되는 웹 2.0의 특징에 대해 설명하고, 3장에서는 제안 시스템 설계를 그리고 4장에서는 제안시스템의 구현 및 실험에 대해 설명하고 마지막으로 결론 및 향후 연구 방향에 대해 논의한다.

2. 관련 연구

2.1 DNS

도메인 네임 시스템(Domain Name System, DNS)은 호스트의 도메인 이름을 호스트의 네트워크 주소로 바꾸거나 그 반대의 변환을 수행하도록 호스트 이름과 IP 주소를 매핑시켜주는 거대 규모의 분산 네이밍 데이터베이스 시스템이다. DNS는 도메인 네임 공간(Domain Name Space)과 네임서버(Name Server), 리졸버(Resolver)로 구성된다. 인터넷의 모든 도메인은 ROOT라 불리는 도메인 이하에 역트리(Inverted Tree) 구조로 계층적으로 구성된다. ROOT 도메인 바로 아래의 단계를 최상위 도메인(TLD, Top Level Domain)이며, 2단계 도메인(SLD, Second Level Domain)은 2단계 도메인 아래에서는 각각의 ISP(Internet Service Provider)가 운용하는 Recursive DNS서버가 운용되고 있다. 이러한 Recursive DNS서버는 일종의 Cache서버 및 다른 TLD나 SLD의 주소를 사용자에게 알려주는 역할을 한다. 이때 리소스 레코드를 이용하게 되는데 보통 해당 도메인 네임과 IP 주소를 매핑하여 놓은 zone 파일을 사용하여 해당 도메인 네임이 가지는 속성 정보를 사용하며 타입에 따라 질의/응답의 형태가 달라진다. <Table 1>은 DNS서버에서 사용하는 리소스 레코드 종류를 나타낸다. 대부분의 DNS의 경우 초기 설정 이후 큰 문제가 발생되지 않는다면 설정을 거의 변경하지 않기 때문에 다양한 형태의 보안 취약점이 발견 될 수 있으며, DNS 보안 위협으로는 DNS 스푸핑(Spoofing) 취약점, DDoS(Distribute Denial of Service, 분산 서비스 거부) 취약점, DNS 프로그램 취약점, 관리적인 취약점 등이 있다.

〈Table 1〉 DNS Type

Type	Value (Dec)	Function
A	1	used to map hostnames to an IP address of the host.
NS	2	Delegates a DNS zone to use the given authoritative name servers.
MX	15	Maps a domain name to a list of message transfer agents for that domain.
SOA	6	Specifies authoritative information about a DNS zone.
PTR	12	Pointer to a canonical name.
CNAME	5	Alias of one name to another.

2.2 DNS 스푸핑

DNS 스푸핑은 실제 DNS 서버보다 빨리 공격 대상에게 DNS Response를 보내, 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도하는 공격이다. DNS 스푸핑 공격은 웹 스푸핑과 비슷한 의미로 이해되기도 한다. 인터넷 익스플로러에 사이트 주소를 입력하여 원치 않는 불법적인 사이트로 연결되는 경우가 있다. DNS 서버의 오류로 인해 발생하는 경우도 있지만 DNS 스푸핑과 같은

공격으로도 발생하는 경우도 있다. 공격자가 DNS 클라이언트와 동일한 LAN 영역에서 패킷을 수동적으로 도청하다가 DNS 요청이 일어나는 시점을 탐지하고, 실제 DNS 서버의 응답이 도달하기 이전에 DNS 응답을 생성하여 공격 대상에게 응답해주는 방법이다. 특히, DNS 패킷은 UDP 패킷이므로 세션이 존재하지 않는다. 또한 웹 브라우저는 자신이 요청한 DNS 응답 중 먼저 도착한 응답 패킷을 신뢰하며, 이어서 오는 두 번째 응답 패킷은 무시한다. DNS 프로토콜의 통신에서 무결성 및 인증과정이 취약함을 나타낸다[3].

2.3 DDoS

DDoS 공격은 여러 대의 좀비 PC가 공격 목표 호스트로 대량의 네트워크 트래픽을 생성시켜 대상 호스트의 네트워크 서비스 기능을 일시적 또는 완전히 정지시키는 공격이다. DDoS 공격의 큰 피해자가 될 수 있는 곳이 DNS이다. DNS에 장애가 발생하면 웹이나 메일을 포함한 모든 도메인 서비스가 중단되어 엄청난 장애가 유발될 수 있다. 대표적인 DNS 공격 형태로는 DNS 플러딩 공격(Flooding Attack), DNS 증폭 공격(Amplification Attack) 등이 있다. 또한 DDoS 방어 기법도 IPS 라우팅, DNS-Sink-Hole, Entropy와 Chi-Square 알고리즘[4], 통계 기법[5], 데이터 마이닝 기법[6,7,8] 등 다양한 방법이 연구되었다.

2.3.1 DNS 플러딩 공격

DNS 플러딩 공격은 주어진 zone에 속한 하나 이상의 DNS 서버를 타겟으로 주어진 zone과 sub-zone 영역에서의 리소스 레코드의 hamper resolution을 시도한다. DNS Flooding Attack은 정상 패킷과 동일한 패킷을 무작위로 전송하여 타겟 시스템의 자원을 고갈시켜 공격 경로상의 네트워크 대역폭 자원을 소모시키는 공격이다. 모든 패킷이 한곳으로 집중되는 현상이 발생한다.

2.3.2 DNS 증폭 공격

DNS 증폭 공격은 DDoS 공격의 한 형태이다[9]. 이러한 공격 형태는 DNS 리졸버나 NTP 서버 같은 Open Internet Service를 이용해서 공격 목표로 대량의 패킷을 보내서 DNS 서비스가 정상 수행되지 않도록 한다. DNS 증폭 공격은 UDP 프로토콜로 53번 포트를 사용한다. 초당 1000개 이상의 패킷을 전송한다. 그리고 실존하는 서버에 대한 DNS 질의가 아닌 허위의 질의를 다량 발생시킨다[10,11].

2.4 DNS의 문제점

인터넷 서비스를 제공하는 업체에 있어 외부에 노출되는 정보는 주로 웹 서버와 DNS 서버이다. 지금까지는 대부분 웹서버에 DDoS 공격이 집중되었으나 점차 DNS에 대한 공격이 집중되고 있다. 웹 서버에 대한 대응체제가 많이 갖춰진 반면 DNS 서버는 DDoS 공격에 노출되어 있다. 첫째, DNS는 UDP 프로토콜과 53번 포트를 사용하기 때문에 웹과 달리 UDP Flooding에 대해 백본에서 ACL로 필터링하는 것이 불가능하다. 둘째, DNS 서버의 초당 처리 가능한 질의의 수에는 한계가 있다. 셋째로, 웹서버는 DNS를 통해 쉽게 IP 변경이 가능하지만, DNS는 자신의 IP를 변경하면 whois를 통해 정보 변경을 해야 할 뿐 아니라 국제 도메인의 경우 변경 내역이 반영되기까지 수일이 걸리다. 넷째로, 한 DNS 서버에 여러 개의 도메인을 세팅해서 운영하거나, 호스팅 업체에서 수만개 이상의 도메인을 한꺼번에 서비스하는 경우에는 DDoS 공격이 발생하여 수시간 동안 DNS 서비스가 정상 작동하지 않으면 그 피해는 엄청나다. 다섯째로 DNS 트래픽은 구조가 단순하여 정상과 비정상 트래픽을 구분하기가 어렵기 때문에 공격에 대해 차단하기도 어렵다. 마지막으로, DNS 공격에 대한 경험과 지식이 전무한 것도 큰 문제이다[12,13].

2.5 Web 2.0

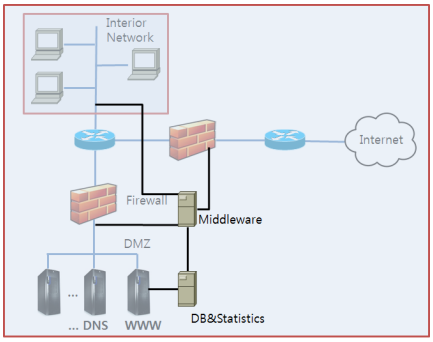
웹 2.0은 O'reilly 사와 MediaLive사의 컨퍼런스 과정에서 탄생한 단어로, 이전의 웹과 단절된 것이 아니라 연속성을 가진 형태에서 웹의 진화 환경에 대해 이야기하는 도중 도출되었다. 웹 2.0은 단순한 웹사이트의 집합체를 웹 1.0으로 보고, 웹 애플리케이션을 제공하는 하나의 완전한 플랫폼으로의 발전을 웹 2.0이라고 지칭한다. 웹 2.0이 구현되어 나타나는 대표적인 형태로는 블로그, 위키, Bit Torrents, Creative Commons, Google, IPO, RSS, Social Software, Web APIs, REST, XHTML/CSS등이 있다. 특히, Ajax 기술은 콜백을 이용하여 입출력에 관계된 부분을 비동기식으로 업데이트한다[14,15].

3. 시스템 설계

침입탐지 시스템(IDS, Intrusion Detection System)은 크게 호스트 기반의 침입탐지 시스템(HIDS, Host-Based Intrusion Detection)과 네트워크 기반 침입탐지 시스템(NIDS, Network-Based Intrusion Detection)으로 나뉜다. HIDS는 전체적인 네트워크에 대한 침입탐지는 불가능하며 스스로가 공격 대상이 될 때만 침입을 탐지할 수 있다. 반면 NIDS는 하나의 독립된 시스템으로 운영되며 감사와 로깅을 할 때는 네트워크 자원 손실이나 데이터 변조의 위험이 적고 IP를 소유하지 않기 때문에 해커의 직접적인 공격에 피해를 입을 걱정이 없는 반면, 공격에 대한 결과를 알 수 없고 암호화된 내용을 검사할 수 없기 때문에 상호 보완적으로 시스템을 구축하는 것이 일반적이다.

3.1 시스템 설계

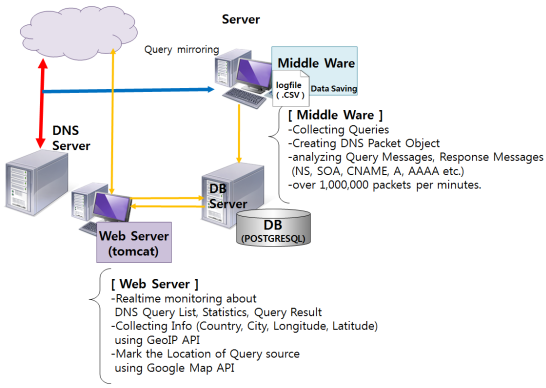
본 논문에서는 DNS 서비스를 이용한 다양한 보안 위협을 예측 및 대응할 수 있도록 HIDS와 NIDS를 상호 보완적으로 시스템을 구축하여 DNS 질의 및 응답을 수집하고, 수집된 데이터를 기반으로 실시간 지도 표현 및 통계 데이터를 표현함으로써 DNS 서비스를 이용한 침해사고 관련 정보를 사전 분석하여 대응할 수 있는 실시간 모니터링 및 제어 시스템을 제안한다.



[Fig. 1] System Architecture

제안 시스템의 구조는 [Fig. 1]과 같다. 내부 라우터에서 DMZ의 DNS에 IN/OUT 되는 트래픽을 TAP 장치를 이용하여 미들웨어를 탑재한 서버로 미러링한다. 미들웨어는 데이터를 수집하고 필터링하는 역할을 수행한다. 통계 정보를 데이터베이스 서버에 저장하고, 저장된 정보는 웹서버에 의해 통계 정보와 함께 DNS 질의와 관련한 지도 정보를 GUI 기반으로 실시간 서비스한다.

[Fig. 2]는 전체 시스템에서 DNS 질의와 DNS 응답 관련한 정보를 실시간 모니터링 하도록 미들웨어, 데이터베이스, 웹서비스를 중심으로 기능적 설계를 나타내며. DNS 서버는 기존의 기능을 그대로 수행한다. 트래픽으로 인한 부하와 데이터 분석 및 처리에 대한 부하를 분산시키도록 데이터베이스 서버는 별도의 시스템으로 구축하여 각종 통계 자료가 저장되도록 한다.



[Fig. 2] Realtime DNS Query Monitoring System

3.1.1 미들웨어

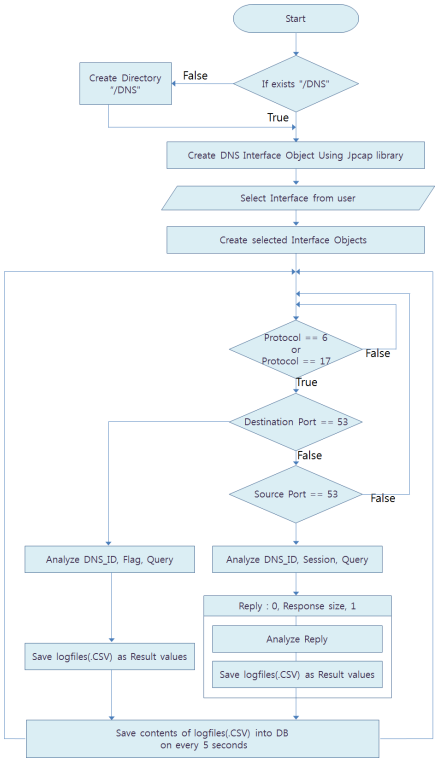
미들웨어는 TCP/IP 패킷을 캡처하여 53번 포트를 사용하는 DNS 질의 요청/응답을 수집하여 분석 및 처리한다. DMZ 영역의 DNS 서버로 IN/OUT 되는 DNS 질의 요청/응답을 탭을 이용하여 미들웨어를 탑재한 서버로 전송되도록 하고 미들웨어는 전송된 데이터를 캡처한다.

TCP/UDP 헤더를 읽어 포트번호가 53번인 경우 DNS 패킷 객체를 생성한다. 질의 메시지와 응답 메시지를 구분하고 NS, SOA, CNAME, A외에는 필터링을 수행한다.

[Fig. 3]은 DNS 질의 요청/응답을 분석하고 저장하기 위한 알고리즘을 나타낸다. Jpcap 라이브러리를 이용하여 인터페이스 객체를 생성하고 다수의 인터페이스로부터 수신되는 패킷을 분석한 뒤 필요한 내용을 CSV 파일로 저장한다.

내부 네트워크에서 캡처되는 DNS 응답 패킷이 DMZ에서 캡처한 DNS 응답 패킷 리스트에 존재하지 않으면 DNS 스푸핑이 발생했음을 감지한다. DNS 플러딩 공격

이 발생하는 경우 DNS 질의 카운터가 임계 수치를 초과하면 방화벽의 필터링 정보를 갱신하여 특정 질의에 대해 필터링 한다. 또한 DNS 증폭 공격은 실존하지 않는 DNS에 대해 대량의 질의가 들어오기 때문에 GeoIP API를 활용하여 존재하지 않는 도메인에 대한 질의를 수행하는 비정상질의를 파악하고 내부 필터링 정보에 포함하여 필터링을 수행한다.



[Fig. 3] Algorithm for analyzing and saving information related DNS Query

3.1.2 데이터베이스

데이터베이스는 수집된 DNS 질의에 대해 분석 영역과 저장 영역을 나누어 저장한다. 각종 분석에 필요한 통계 자료를 저장하여 필요에 따라 검색 가능하도록 저장한다. 미들웨어에서 수집한 질의에 대해 카운터와 함께 새로운 테이블에 일정 주기로 저장하여 주기별 평균, 최대치, 초당 DNS 질의 전체 카운터 등 통계치를 산정할 수 있도록 설계하였다.

3.1.3 웹 서비스

데이터베이스에 수집 저장된 데이터는 웹을 통해서 DNS 질의/응답 내용을 실시간으로 확인이 가능하다. 웹 페이지는 DNS Query 리스트, 통계치 등의 정보를 나타내며, 결과를 실시간으로 확인가능하도록 Ajax 기술을 이용한다. 또한 GoeIP를 통해 쿼리의 국가, 도시, 지역, 위도, 경도 정보를 수집하여 구글맵 API를 통해 질의 발생지를 지도상에 실시간으로 표시하도록 설계하였다.

4. 시스템 구현 및 실험

본 논문에서 제안하는 시스템은 CentOS6.4 기반의 리눅스 서버에 미들웨어를 탑재하였다. libpcap, jpcap 패킷 캡처 라이브러리를 사용하였으며 개발 언어는 Java 이다. 성능평가는 Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz × 2에 메모리 4G의 저가형 PC에서 수행하였다. 데이터베이스는 오프소스 DBMS인 PostgreSQL을 사용하였다. 기존의 INSERT 방식의 데이터베이스 저장은 패킷의 로스트가 많아 COPY 방식으로 구현하였으며 분당 30만건 이상의 데이터를 처리하며 기존의 방식에 비해 월등하다는 것을 <Table 2>를 통해 알 수 있다. <Table 2>는 미들웨어의 성능을 평가한 결과이다.

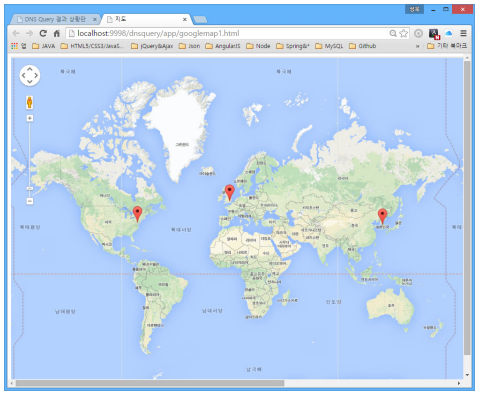
〈Table 2〉 Comparison of Performance

packets/m (10 times)	method1(INSERT)		method2(COPY)	
	normal packets (average)	lost packets (average)	normal packets (average)	lost packets (average)
1,000	1,000	0	1,000	0
3,000	3,000	0	3,000	0
5,000	4,983	17	5,000	0
10,000	6,956	2826	10,000	0
30,000	7,174	22826	30,000	0
50,000	7,281	42719	50,000	0
100,000	7,578	92422	100,000	0
300,000	8,122	291878	300,000	0

웹 서버는 아파치 톰캣과 스프링 프레임워크를 사용하였으며, 클라이언트 기술로는 JQuery, Ajax를 이용하였다. [Fig. 4]는 DNS Query 결과를 실시간으로 모니터링하는 페이지를 나타낸다.

[Fig. 4] DNS Query Data

[Fig. 5]는 DNS 질의 결과를 GeoIP API를 이용하여 DNS패킷 발생지의 정보(국가코드, 도시이름, 위도, 경도, 유해 DNS 식별)를 나타내며 Google API를 이용하여 지도상에 그 위치를 나타낸다. GeoIP에서 검색되지 않는 정보는 DNS 증폭 공격에서 사용되는 허위 질의이거나 내부 사용자에 의한 불법적인 사이트 접속일 경우 이므로 방화벽의 필터링 정보로 활용한다.



[Fig. 5] DNS Query Mapping with locations from GeoIP using Google API

내부 네트워크와 DMZ의 DNS 응답 패킷이 일치하는지의 여부에 따라 스프핑 발생여부를 확인한다. 즉, DMZ에서 전송하지 않는 DNS 응답 패킷이 내부 네트워크에서 발생하면 그 즉시로 스푸핑 발생 여부를 확인할 수 있다. 향후 사전 차단 방법의 연구가 필요하다.

5. 결과 및 향후 연구

본 논문에서는 DNS를 이용한 외부의 보안 침해 공격이나 내부의 불법적인 DNS 질의에 대해 실시간으로 모니터링하고 제어할 수 있는 실시간 DNS 질의 모니터링 시스템을 제안하였다.

기존의 특정 문제만을 해결하기 위한 시스템에 비해 제안 시스템은 DNS 스푸핑, DNS 플러딩 공격, DNS 증폭 공격 등 다양한 공격에 대응할 수 있으며, 불법적인 DNS의 사용을 미리 차단함으로써 내부로부터 발생할 수 있는 불법적인 침해 사고를 예방할 수 있다. 웹으로 실시간 정보를 확인함으로써 언제 어디서든 관리가 가능한 시스템이다.

제안 시스템에서 탭을 통해 수집되는 데이터나 DDoS의 공격을 받는 시스템은 대부분 일시적으로 급격히 증가하는 패킷수의 카운터에 의해 처리되기 때문에 향후 좀 더 효율적이고 효과적인 DDoS 대응이 가능하기 위해서는 빅데이터 처리 기법을 이용하여 처리능력 및 성능을 고도화 할 필요가 있다. 특히 하둡 같은 분산 환경의 데이터 처리와 저장을 쉽게 할 수 있는 시스템을 도입하여 DDoS 등의 공격에 더욱 빠르게 대처해야 할 필요가 있다.

REFERENCES

[1] Ji-Woo Choi, Myung-Jin Chun, Do-Won Hong and Chang-Ho Seo, “A Proposal Countermeasure to DDoS attacks targered DNS”, Journal of JKIISE, Vol. 23, No. 4, pp. 729-735, August 2013.

[2]http://biz.chosun.com/site/data/html_dir/2014/04/25/2014042501090.html

[3] DaeHee Chang, YoungSu Park, “DNS Spoofing Protection System for Wi-Fi Networks”, Journal of KIISE : Computing Prantices and Letters, Vol. 18, No. 5, pp. 429-433, 2012.

[4] D. Moore, G. M Voelker, and S. Savage, “Infferring, Internet Denial-of-Service Activity,” The 2001 USENIX Security Symposium, 2001.

[5] Feinstein L., Schnackenberg D, Balupari R., Kindred D., "Statistical Approachs to DDoS Attack Detection

and Response“, DARPA information Survivability Conference and Exposition(DISCEX 2003), April 22-24, 2003.

[6] JungHyun Kim, Soohan Ahn, Youjip Won, Jongmoon Lee, Eunyung Lee, “Detectio of Traffic Anomalities using Mining : An Empirical Approach” Journal of KIISE Vol. 33, No. 3, pp. 201-217. June. 2006.

[7] A. Lakhina, M. Crovella, and C. Diot, “Diagnosing Network-Wide Traffic Anomalies,” ACM SIGCOMM 2004, 2004

[8] A. Lakhina, M. Crovella, and C. Diot, “Mining Anomalies Using Traffic Feature Distributions” ACM SIGCOMM 2004, 2004

[9] http://technet.microsoft.com/en-us/security/hh972393

[10] YE, Xi, and Yiru YE. “A Practical Mechanism to Counteract DNS Amplification DDoS Attacks.” Journal of Computational Information Systems 9:1, pp. 256-272. 2013.

[11] Wei-min, Li, Chen Lu-ying, and Ley Zhen-ming. “Alleviating the impact of DNS DDoS attacks.” Network Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on. Vol. 1. IEEE, 2010.

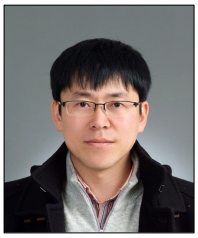
[12]http://www.dailysecu.com/news_view.php?article_id=194

[13] The Measurement Factory DNS Survey: dns_survey_2010.pdf

[14] Pilgu Kang, Jaehwan Kim, Jinseok Chae, Sangjun Lee. “A Design and Implementation of RSS Data Collecting Engine based on Web 2.0”, Journal of Korea Multimedia Society Vol. 10, No. 11, pp. 1496-1506, Nov 2007.

[15] Joshua Hailpern, Loretta Guarino Reid, Richard Boardman, Srinivas Annam, "WEB 2.0: Blind to an Accessible New World," ACM, May, 2007.

장 상 동(Jang, Sang Dong)



- 1997년 2월 : 경남대학교 전산통계학과(이학사)
- 1999년 2월 : 경남대학교 컴퓨터공학과(공학석사)
- 2005년 2월 : 경남대학교 컴퓨터공학과(공학박사)
- 2012년 3월 ~ 현재 : 경남대학교 컴퓨터공학과 교수
- 관심분야 : 모바일 컴퓨팅, 사물인터넷, 컴퓨터보안,
- E-Mail : angong@kyungnam.ac.kr