TCP/IP Layer별 공격패턴 분석에 기반한 CFC를 이용한 DDoS 방어 알고리즘 연구

서 우 석* · 박 대 우** · 전 문 석***

A Study on the DDoS Defense Algorithm using CFC based on Attack Pattern Analysis of TCP/IP Layers

Seo, Woo Seok · Park, Dea Woo · Jun, Moon Seog

〈Abstract〉

Paper is on defense for so-called internet crisis, the attack of DDoS (Distributed Denial of Service) which was targeted to the central government ministries, financial sector, and portal sites of chief counties including Korea on June 7th, 2009 as its start. By conducting attack with various DDoS attacking methods in the lab environment and dividing networks targeted by the attack by layers, this paper records and analyzes the chief information for attack, destination information of packets, defense policy setting, and the flow of packet attack with the subjects of the networks separated. This study suggests CFC system using multiple firewalls applying defense policy corresponding to the target layer for ultimate attack and tests it according to the result of analyzing the attack packet information and its amount, log analysis, access recording port, and MAC and IT information, etc. by layers. This article is meaningful in that it analyzes the attack by layers, establishes firewall policy for protecting each layer, and secures accurate mechanism for detect and defense.

Key Words : DDoS(Distributed Denial of Service), Security Policy, CFC(Choose firewall channel), Defense method, TCP/IP Layer

Ⅰ. 서론

공중망에서 사이버 공격방법이 다양한 정책과 기술을 기반으로 하는 최신 방어 기술을 무력화 시키는 범위가 특정 목적을 수행하는 시스템에 국한되어지지 않고 2차, 3차에 이르는 전파형태의 공격으로 변형되어지고 있다. 최신 공격 형태를 단계별로 분석하면, 1단계는 특정 시스템 서비스 장애를 발생시키고 2단계는 공격을 받은 시스템이 동일 네트워크 또는 공개되어진 네트워크상에 불특정 다수의 시스템을 공격하는 Zombie로 변형되어지는 것이다. 최종 3단계로는 최초 공격 시스템 정보와 네트

* 숭실대학교 일반대학원 컴퓨터학과 박사과정
** 호서대학교 벤처전문대학원 IT응용기술학과 조교수(교신저자)
*** 숭실대학교 일반대학원 컴퓨터학과 정교수

워크 이용경로 및 공격기법 등의 정보를 소멸시킴으로써 네트워크상에 존재하는 주요 시스템 침해를 유발시키고 증거인멸을 하는 상황이다[1].

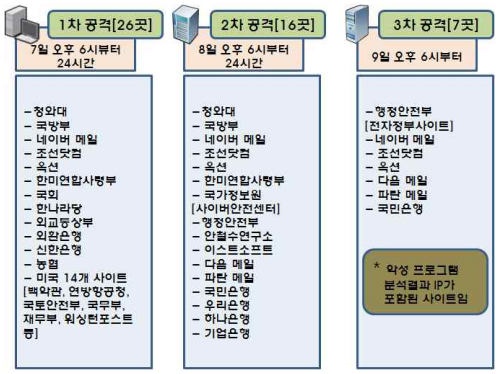
DDoS 공격으로 사회전반에 걸친 경제적인 손실과 정보의 유출이 얼마나 큰 문제점을 야기하는지를 확인한바 있으며, 이러한 침해로 인한 문제점 발생을 최소화하고 빠른 대처방안을 연구해야 한다. 본 논문에서는 최근 이슈가 되어진 7.7 인터넷 대란에 사용되어진 공격기법을 분석할 필요가 있으며, 또한 학술적인 차원에서 DDoS 공격에 대한 공격기법을 연구하여 체계적으로 분류하고, 분류된 DDoS 공격기법에 따른 방어기법을 연구하여야 하며, 연구된 내용의 실험을 통해 DDoS 공격방어 체계 구축을 연구할 필요가 있다.

본 논문에서 제안하는 TCP/IP Layer별 DDoS 공격을 방어하는 기법을 CFC(Choose Firewall Channel, 이하 CFC라 한다.)라 정의하고 CFC를 이용해 계층별 공격기법과 방어기법을 분리하고 계층 간 공격성향에 맞추어 DDoS 공격과 방어기법에 대한 실험과정과 분석결과를 기술한다. 본 논문의 구성은 다음과 같다. 2장에서는 DDoS 공격 사례와 TCP/IP Layer별 DDoS 공격 분류를 확인하고 3장에서는 TCP/IP Layer별 DDoS 공격방법과 방법 기법을 연구하고 그 기능들이 기술되고, 4장에서는 TCP/IP Layer별 DDoS 공격에 대한 방어 실험을 하고, 5장에서는 결론과 향후연구를 기술한다.

Ⅱ. 관련연구

2.1 DDoS 공격 사례

7.7 인터넷 대란은 DDoS 공격을 체계적이고 짧은 기간에 빠르고 정확하게 특정한 주요기관을 집중 공격함으로써 <그림 1>과 같이 국가정보망과 금융권 및 포털 사이트의 서비스를 차단시켰다. 이처럼 7.7 인터넷 대란에서 주요 국가 전산망에 문제를 발생시켜 사회적인 보안에 대한 인식의 변화를 가지고 왔다. 이후 DDoS에 대한 새로운 방어기법들과 솔루션이 난무하고 있으며, DDoS의 공격을 정확하게 차단하고 제공하는 서비스를 지속가능하도록 하는 솔루션은 아직도 제안되어지지 못하고 있다[1,2].



<그림 1> 일자별 DDoS 공격 대상

기존에 보안부문에서 인식하고 적용했던 방어 전략과 기능은 모두 금번 공격으로 차단이 불가능함을 확인했으며, 공격방법이 서비스만을 거부토록 하는 단계에서 다단계적으로 1차 공격, 2차 확산, 3차 증거인멸로 세분화되어 공격이 이루어졌다[3].

2.2 TCP/IP Layer별 DDoS 공격 분류

DDoS 공격 유형을 사전에 TCP/IP Layer별로 분류하고, 분류되어진 TCP/IP Layer별로 공격 가능한 패턴을 사전에 분석함으로써 최초 공격이 이루어짐과 동시에 <표 1>과 같이 TCP/IP 및 OSI7 Layer별 방법 기법을 적

<표 1> 계층별 공격대상

OSI	TCP/IP	전송단위	주소체계	주요장비	공격유형
Application	Application	Message	Domain name	PC	Virus, Worm, 트로이목마, 버퍼오버플로우, OS 및 Application 취약점 공격
Presentation					
Session					
Transport	Transport	Segment Datagram	Port Address	L4 Switch	TCP Syn Flooding, UDP Flooding 등
Network	Internet	Packet	IP Address	Router, L3 Switch, IP Sharing	IP 변조, DHCP 공격, ICMP 공격
DataLink	Network	Frame	MAC	Switch, Bridge	MAC Flooding, MAC 변조, ARP 공격
Physical		Bit/signal		Hub, Repeater	케이블 단절

용함에 따라 DDoS 공격을 체계적으로 방어가 가능하다[4].

Ⅲ. TCP/IP Layer별 DDoS 공격방법과 방어기법

DDoS 공격과 TCP/IP Layer와의 연관관계에 따라서 해당 TCP/IP Layer에 준하는 공격방법과 해당 기술을 분리하여 공격 형태와 결과 그리고 공격방법과 방법기법을 <표 2>와 같이 분석하였다[5,6,7].

<표 2> 공격 분류와 분류에 따른 방어기법

구분	공격분류	방어기법
Application	HTTP Get Flooding / Cache Control Attack / VoIP Attack / SQL Attack / RPC Attack / Botnet Worm and Hacking	Realtime Application Content Filtering / 지능형 학습 기반의 필터링 / 리얼타임 이벤트 패턴 매치 필터링
Transport	TCP SYN Flooding / TCP RST Flood Attack / TCP ACK Flood Attack / UDP Flooding	보안정책 위배 패킷 보안 / 보안정책 위배 포트 보안 / 보안정책 위배 데이터베이스 보안
Internet	IP Spoofing / ARP / RARP Flooding / IGMP Spoofing	패킷 필터링 / IP 검출과 차단
Network	MAC Flooding / MAC modulation	MAC Flooding과 변조 방지 / ARP 공격 차단

3.1 TCP/IP Layer별 DDoS 공격방법

3.1.1 Application Layer 공격

(1) HTTP Get Flooding

TCP/IP Layer 최상위 계층인 Application 계층을 주요 공격대상으로 하고 네트워크상의 연결성을 대상으로 하는 DDoS 공격과는 달리 프로그램적인 면이 다소 강한 공격으로 공격 툴 역시 공격자의 공격목적과 의도가 충분히 반영된 공격알고리즘을 기반으로 작성되어진 것이다. Network 계층의 물리적인 연결에 대한 공격보다 지능화된 HTTP Layer 등을 분석과 동시에 공격함으로써 웹 부하공격 GET Flood(HTTP GET)과 CC(Cache Control) 공격을 한다. Application 계층의 공격방법으로는 HTTP 웹 서버 Scanning 및 request DDoS 공격 등이 있다. HTTP의 연결요청에 의한 서비스다운 공격으로 인한 HTTP Flood 인터넷 서비스사이트가 제공하는 웹서비스에 장애를 발생시켜 서비스전체가 차단되거나 서비스를 위한 프로세서인 daemon을 다운 시킨다.

(2) Cache Control 공격

Cache Control 공격목적은 웹서버와 데이터베이스 서버에 부하를 발생시킴으로써 서비스 제공을 차단하는 것이다. 또한 NetBOT DDoS Tool에 의한 CC 공격으로 HTTP user agent header에 Cache-Control 값을 추가하여 웹서버에 전송함으로써 서버의 과부하를 유발하는 공격이다.

(3) VoIP 공격

VoIP 공격은 웹 서버를 연속적으로 호출함으로써 서버를 불능상태에 빠트리는 공격으로 사용자간의 통신 패킷이 발생하거나, 계속적인 요청을 하는 등의 정상적인 서비스를 방해하여 VoIP 사용자간의 원활한 통신을 방해하는 공격이다. 또한, 공격으로 인해 사용자간의 통신 패킷 손실을 발생시켜 통신을 차단한다[8].

(4) SQL 공격

웹사이트들은 사용자로부터 입력받은 값을 이용해 데이터베이스 접근을 위한 SQL query를 구성한다. 이때 사용자가 유효한 계정과 패스워드를 입력했는지 확인하기 위해 사용자 계정과 패스워드에 관한 SQL query문을 구성, SQL injection 기법은 웹 Application 자체의 버그를 이용하는 웹 해킹방법이며, 정상적인 SQL query를 변조할 수 있도록 조작된 사용자 이름과 패스워드를 보내 정상적인 동작을 방해하는 비정상적인 SQL query를 이용하는 공격이다.

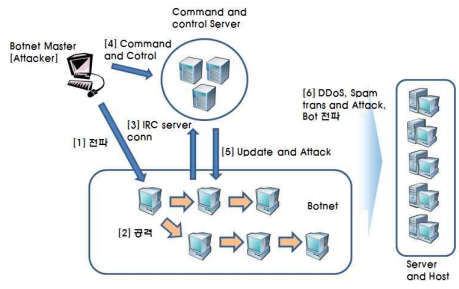
(5) RPC 공격

RPC(Remote Process Control) 서버는 서버가 수신한 내

용을 검증하는 과정이 없기 때문에 접근한 클라이언트로부터 잘못된 RPC 패킷을 수신할 경우, 정상적인 RPC 요청에 대해서는 응답할 수가 없는 장애가 발생하는데, 이러한 비정상적인 RPC 패킷을 대량으로 서버에 전송함으로써 서버의 서비스를 중단시키는 공격이다. 또한, 내부 포트로 공격을 해서 서버내부에 버퍼오버런을 발생시키기도 한다.

(6) Botnet Worm and Hacking

Internet 계층과 Network 계층 전반에 걸쳐 공격이 가능한 DDoS 공격방식이며, Application 계층에까지 그 영향이 미친다. 지능적이고 자동화된 강력한 툴과 인터넷 상에서 공격자들의 공격 알고리즘 배포 등으로 인터넷 접근이 가능한 누구나 쉽게 공격자로 돌변할 수 있다. <그림 2>와 같이 Botnet 공격이 이루어지며, 또한, Botnet은 Bot, Botmaster, C&C서버로 구성되어 명령에 따라 제어할 수 있는 Zombie 네트워크를 의미하며, 일반적으로 수백 대에서 수천대로 구성된 원격으로 제어되는 Zombie 시스템으로서 IRC, HTTP 또는 P2P에 의해서 제어된다. 또한, 감염된 시스템 소유자는 감염 사실을 인지할 수 없고 탐지가 어렵다. 또한 계층 간에 접근 기술 부문의 융통성과 호환 알고리즘을 지닌 공격에 이용되어진다. Botnet을 이용한 다중혼합 공격으로 TCP SYN Flood, UDP Flood, ICMP Flood 등을 혼합한 공격을 공격 대상 시스템으로 무작위로 보내는 방법을 이용하는 공격 등이 있다.



<그림 2> Application 계층의 DDoS 공격 형태 – Botnet worm과 Hacking

3.1.2 Transport Layer 공격

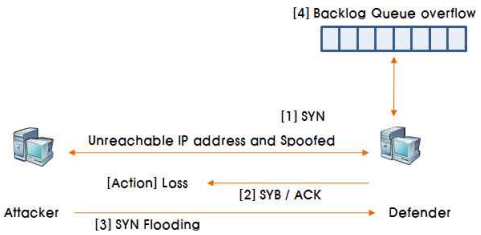
(1) TCP SYN Flooding

공격자는 TCP SYN 패킷을 무작위로 공격대상 장비에 순간 전송 패킷 량을 급증시켜 수신측의 TCP 세션을 받는 listen queue 공간을 overflow시켜 정상적인 세션의 연결을 차단하고, 시스템은 무차별적으로 들어오는 TCP 세션으로 인해 시스템 장애가 발생 마비되는 공격으로 일반적인 공격방법 중에 하나이며, TCP/IP Layer의 Transport 계층을 그 주요 공격 계층으로 한다.

주요 공격 형태는 Non 스푸핑 공격(봇넷 동반 공격), 스푸핑된 공격, 봇넷 등과 같이 다양한 공격 형태가 있으며, <그림 3>에서와 같이 클라이언트에서 서버에 접속을 요청하는 SYN 패킷을 보내고 서버는 ACK 패킷과 SYN 패킷을 클라이언트에 보냄으로써 다시 클라이언트가 서버에 ACK 패킷을 보내야 연결이 이루 지는데 몇몇 해커들은 가짜 IP를 사용하여 SYN을 보내고 ACK, SYN을 받고 ACK를 보내지 않음으로써 서버측은 ACK를 받을 때까지 대기상태가 되고 백로그 큐라는 메모리 공간에 로그가 계속 기록되는데, 메모리가 다 차면 더 이상의 연결을 받아들일 수가 없게 됨에 따라 해당 포트로는 연결을 할 수가 없게 되는 것으로 수신거부상태가 된다. 또한, TCP 3-way Handshake에서 발생 하는 것이므로 Transport 계층의 프로토콜인 TCP를 공격하며, 3-way Handshake를 하기 위해선 A에서 B로 SYN을 보내고 (SYN Sent상태-query) B에서 A로 SYN+ACK을 보내주면 (SYN Receved-response) A는 다시 ACK를 보내줘야 하는데 이 단계에서 A가 ACK을 보내지 않는 것이다. 이 공격은 Port만을 대상으로 장애를 유발하고 다른 서비스 즉, Application 계층에는 영향을 주지 않는다.

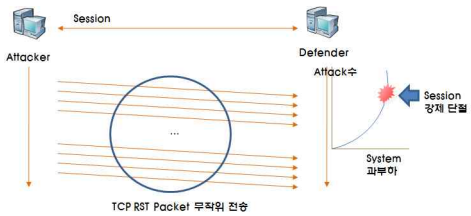
(2) TCP RST Flood 공격

공격자가 특정 시스템에 접근하여, 시스템 간 세션을 연결 후에 <그림 4>와 같이 TCP RST 패킷을 지속적으로 무작위로 전송함으로써 한계 이상의 세션유지를 위한



<그림 3> Tranport 계층의 DDoS 공격 형태 – TCP SYN Flooding

action 세션을 차단 및 단절시켜 특정 시스템의 Transport 계층의 세션부문을 무력화 시키는 DDoS 공격의 일종이다. TCP SYN Flood 공격과 동일한 세션 상에서 TCP 프로토콜을 통한 세션 연결시의 기능상의 action인 RST를 공격하는 방법이다.



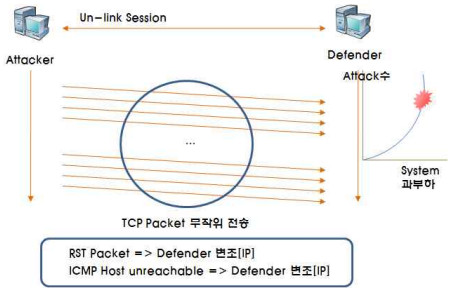
<그림 4> Transport 계층의 DDoS 공격 형태
– TCP RST Flooding

(3) TCP ACK Flood 공격

TCP ACK Flood 공격은 <그림 5>처럼 공격 형태로 구성되며, TCP 세션의 연결을 위한 방법 중에 특정 기능인 ACK를 이용하여 공격자가 TCP 세션이 없는 상태에서 TCP ACK 패킷을 무작위로 보내면 수신측에서 변조된 송신IP로 RST 패킷을 무작위로 보내게 되고, 동시에 ICMP host unreachable 패킷을 보내면서 수신측 시스템의 과부하를 초래하는 공격이다.

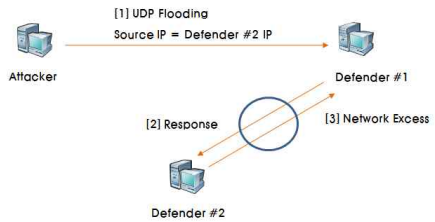
(4) UDP Flooding

Transport 계층의 프로토콜 중에 하나인 비연결성 프로토콜인 UDP를 이용한 DDoS 공격이며, <그림 6>과 같이 UDP 공격은 악성 IRC Bot Flooding 공격과 유사한



<그림 5> Tranport 계층의 DDoS 공격 형태 – TCP ACK Flooding

유형으로 악성 Zombie 시스템을 이용해 대량의 트래픽을 부가시키는 공격으로서 DDoS 공격방법으로 급부상하고 있다. 또한, 공격자는 UDP 패킷을 다량으로 유발시켜 네트워크 대역폭을 소모시키는 공격의 하나이며, 비연결성 프로토콜로 query와 response가 필요 없지만, 일반적인 단방향의 공격자의 연결 요구와 제어 및 데이터 전송으로 과부하가 발생되어 장애를 유발하는 공격이다. UDP 패킷을 다량으로 유발시켜 네트워크 대역폭을 소모시키는 공격으로 지원 서비스를 다운 시킨다.



<그림 6> Transport 계층의 DDoS 공격 형태 – UDP Flooding

3.1.3 Internet Layer 공격

(1) IP Spoofing

네트워크상에 상호 신뢰관계인 서로 다른 시스템 A, B 두 시스템 간에는 A 시스템의 어카운트를 가지고 B 시스템을 액세스 할 수 있다. 이 두 시스템 간에는 Trust-membership을 구성, 상호 요구하는 서비스가 IP를 기반으로 인증을 하는데, 이때 상대방 시스템인 A 또는

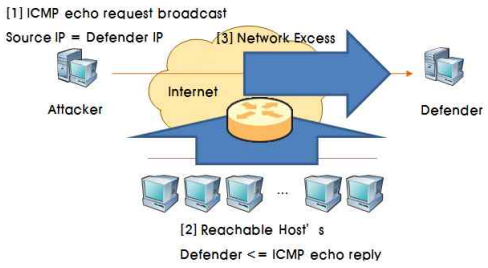
B로 위장하여, 공격자 시스템을 신뢰관계에 있는 시스템인 것처럼 속여, 공격하는 방법이다[9].

(2) ARP / RARP Flooding

ARP 프로토콜은 미인증 프로토콜로써 ARP reply 패킷을 각 호스트에 보내서 쉽게 ARP cache를 업데이트시킬 수 있다. 이때 네트워크상의 시스템들에게 위조 또는 변조한 MAC address를 전송하여, 다른 시스템의 ARP cache를 업데이트시킨다. cache내의 주소가 reflash되기 전에 계속적으로 변조된 ARP reply를 보내므로 네트워크상의 다른 시스템들은 ARP cache의 변조된 MAC 주소의 정보는 계속 유지한다. 이때 공격하는 방법이다.

(3) ICMP Flooding

Internet 계층을 공격 대상으로 하는 공격으로 공격자는 ICMP Echo request를 무작위로 보내어 수신측이 다량의 ICMP Echo reply하게 함으로써 <그림 7>과 같이 시스템의 부하를 유발시키는 DDoS 공격방법으로 매우 흔하고 쉽게 발생시킬 수 있는 공격이다. Ping 같이 특정 시스템에 대한 송수신 가능 상태를 확인 하는 명령을 무작위로 지속적으로 응답을 요구하는 형태와 같은 방법을 이용한다.



<그림 7> Network(Internet) 계층의 DDoS 공격 형태 – ICMP Flooding

(4) IGMP Spoofing

스위치가 모든 IGMP에 대한 reply를 위한 Multicast Mac table을 생성하고, 시스템의 IGMP report message를 참조, 시스템이 접속되어 있는 Port의 MAC table을 생성되어지는 부문을 공격하는 방법이다.

3.1.4 Network Layer 공격

(1) MAC Flooding

한 포트에서 수천, 수백 개의 시스템이 스위치와 연결되어 있는 것처럼 변형되어 보이지만, 변조된 MAC 정보를 공격 시스템에서 발생시키는 것이며, 단시간에 대량의 위장된 MAC 주소를 특정 포트에서 발생시킴으로써 스위치가 MAC 주소를 cashing할 때 하드웨어 공간 제약을 발생시켜 MAC 주소 cache를 위조된 MAC 주소로 채워 정상적인 서비스를 저해하는 공격방법이다.

(2) MAC 변조

Frame에 기록되어진 MAC 주소를 속여, 시스템에 접근함으로써 정상적인 시스템으로 전송되는 패킷을 훔쳐 이를 분석해서 공격하는 방법이다.

3.2 TCP/IP Layer별 DDoS 방어기법

3.2.1 Application Layer 방어기법

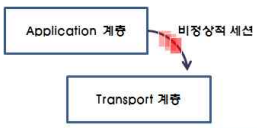
(1) 리얼타임 Application 콘텐츠 필터링

Application 계층에 접근되어지고 운영되어지는 다양한 세션정보를 가진 콘텐츠를 대상으로 필터링 하는 방어기법은 Firewall, IDS, IPS, ESM(Enterprise Secure Management)이 있다. ESM은 연결된 Application 세션을 실시간으로 Virus와 Worm 그리고 Trojan Blocking, Server Protection, Networking - Traffic Management, Spam Mail Blocking 등과 같은 다양한 보안기능을 모두 집약한 보안형태로 통합보안기법으로 운영된다. Application 필터링 이후 불법적이고 비정상적인 접근이 감지되어진 경우 하위 TCP/IP Layer인 Transport 계층

의 1차 방어기법인 보안정책 위배 패킷 보안기법과 연동하여 방어를 구현한다[10, 11].

(2) 지능형 학습 기반의 필터링

지능형 학습기반 필터링은 정상적인 접근 세션과 비정상적인 접근 세션으로 구분하고 각각의 접근 세션을 학습함으로써 별도의 데이터베이스를 구축 및 분류를 한다. Inbound-패킷을 Transport 계층의 접속 Port에서 1차 확인 후 접속한 세션이 정상적인 Port로 접속한 경우는 2차 기존에 학습되어 데이터베이스화 되어진 정보와 비교하고 최종 판단 이후 허용을 한다. 1차 확인 시 비정상적인 공격성 패킷으로 분류 시는 Transport 계층의 방어기법을 적용하여 차단 또는 폐기한다. 지속적이고 연속적인 학습정보의 축적과정과 주기적인 관리가 필수적이며, <그림 8>과 같이 4단계의 보안 단계별 기법을 적용한다. 1단계 비정상적인 패킷에 대한 Transport 계층으로 Forwarding, 2단계 Drop, 3단계 거부, 4 단계 별도의 비정상적인 패킷 누적, 미러링을 통한 접근허용으로 역추적 가능 정보 누적 등으로 구성한다[12, 13].



구분	1단계	2단계	3단계	4단계
보안 단계별 기법	비정상적인 패킷에 대한 Transport 계층으로 Forwarding	Drop	거부	비정상적인 패킷 및 역추적 가능 정보 누적

<그림 8> 보안 단계별 처리기법

(3) 리얼타임 이벤트 패턴 매치 필터링

Application 계층에 접근하는 다양한 이벤트에 대한 접근 패턴과 목적을 분석하고 기존 학습되어진 패턴과 이벤트 패턴 매치 과정을 거쳐서 비정상적인 또는 정상적인 접근인지를 확인하고 접근허용 또는 접근차단을 실시한다. 단, 학습 정보를 비정상 또는 정상적적인 정보 중 기준을 선정하고 지속적인 학습과 정보누적으로 패턴 매치를 위한 기본 정보를 누적한다. 패턴 매치의 결과가 비정상적인 접근인 경우 하위 TCP/IP Layer인 Transport 계층으로 1차 방어기법인 보안정책 위배 패킷 보안기법, 보안정책 위배 포트 보안, 보안정책 위배 데이터베이스 보안 등과 연동하여 방어를 구현한다[14].

3.2.2 Transport Layer 방어기법

(1) 보안정책 위배 패킷 보안

Application 계층에서 방어기법의 하나인 필터링을 통해 콘텐츠와 이벤트 등을 분석하고 이중 필터링 결과에 의해 발생되어진 비정상적인 또는 보안정책에 위배된 콘텐츠와 이벤트 패킷이 발생시 Transport 계층의 포트 컨트롤 방법에 의해 해당 최초 접근 포트를 확인하고 지속적인 또는 비정상적인 패킷의 재유입을 차단하기 위해 TCP/IP Layer에 접근 패킷의 서비스 포트를 재확인하고, 사용되어진 포트를 즉시 차단하고 해당 패킷을 drop함으로써 비정상적인 패킷 접근을 통한 공격을 방어한다.

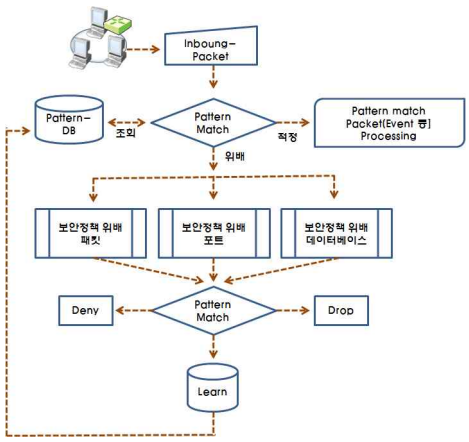
(2) 보안정책 위배 포트 보안

Application 계층에서 운영되어지는 콘텐츠와 이벤트에 대한 보안정책을 기반으로 정책 위배여부에 따른 포트 접근 제어방식의 방어기법이다. Application 계층의 필터링 결과인 콘텐츠 및 이벤트와 Transport 계층의 서비스 포트가 일치 되어야함에도 불구하고 최종 분석결과 해당 서비스가 할당 받아 운영 중인 포트가 전혀 다른 포트를 이용하고 있다면, 불법적인 또는 비정상적인 서비스가 이루어지고 있음으로 해당 서비스를 제공하는 Transport 계층의 서비스 포트 할당을 취소하고 부여한 포트를 회수함으로써 공격을 방어한다.

(3) 보안정책 위배 데이터베이스 보안

<그림 9>처럼 보안정책 기반의 보안은 Application 계층에서 서비스 되어진 콘텐츠 및 이벤트에 대한 1차적인 보안정책 위배 패킷 보안과 2차적인 보안정책 위배

포트 보안 방법을 적용 이후에 콘텐츠 및 이벤트가 공격자의 인위적인 또는 불법적인 접근으로 판명되어진 패킷을 별도의 정책운영 툴을 이용해서 블랙리스트 구성 및 정보를 저장하는 방법의 학습형, 누적형 데이터베이스를 구현함으로써 향후 진입되어지는 패킷의 정보를 분석과 동시에 공격자 판명과 판별에 따른 패킷 재진입 포트를 폐쇄한다. 또한, 데이터베이스를 구성시에 특정 플래그 판별 식별자를 구성함으로써 판별 및 차단에 따르는 접근 시간과 차단시간을 줄일 수 있으며, 정책적용 시간으로 인한 유입되어지는 수많은 패킷의 정체로 인한 과부하도 해소가 가능하다[15].



<그림 9> 보안정책 위배 패킷, 포트, 데이터베이스 필터링 흐름

3.2.3 Internet Layer 방어기법

(1) 패킷 필터링

Internet 계층 망 내에서 목적지로 이동하는 수많은 패킷을 대상으로 원하는 최종 목적지로 Forwarding 하기 위해 서로 다른 패킷으로 캡슐화와 암호화한 패킷들을 분석함으로써 필터링의 역할을 수행하고 불법적인 접근을 방어한다. 또한, 외부 또는 내부 네트워크로부터 접근한 패킷을 분석하여 통과 또는 차단 유무를 판단하고 패킷의 header에서 목적지와 출발지 address를 분석, 확인하여 Forwarding한다. 물리적인 장치로는 라우터와 방화벽 등을 활용하며, 이러한 장비들의 보안정책인 접근과 차단 정책 설정 정보에 의해 불법적인 패킷의 접근을 차단한다[16].

(2) IP 검출과 차단

Internet 계층에서 불법적인 또는 변조되거나 비정상적인 패킷을 검출하고 패킷 필터링 방어기법을 혼용해서 공격을 방어한다. 전송되어진 또는 접근하는 패킷의 구성 정보인 버전, 헤더길이, 전체길이, TTL, 프로토콜, 원격지 IP 주소, 목적지 IP 주소, 데이터 등을 구성 단계별로 분리하고 각 분리되어진 정보를 분석함으로써 공격성 패킷을 차단한다. 패킷 필터링 방어기법과 다소 유사한 방어기법으로 혼용되어지지만 IP 검출의 경우는 패킷을 구성하고 있는 모든 필드 정보를 대상으로 하기 때문에 한 단계 진보된 방법이며, 검출된 결과에 따른 차단 행위를 시행하기 때문에 빠르고 신속한 비정상적인 접근을 제어한다. 따라서 제2, 제3의 공격으로 인한 역속적인 장애를 차단한다.

3.2.4 Network Layer 방어기법

(1) MAC Flooding과 변조 방지

MAC Flooding 공격 형태는 MAC address 자동 생성기 등의 MAC address를 다량으로 생성하여 물리적인 네트워크 연결 장치인 스위치에 대량의 MAC address의 접근을 발생시켜 스위치가 보유한 캐시인 MAC table을 overflow시킴으로써 스위치의 본래의 기능을 상실시키고 허브의 기능만을 유지하게 하여 Promiscuous mode로 설정된 노드의 패킷 정보를 변조 가능하다. 따라서 물리적인 스위치 장비의 포트 보안과 MAC address table의 크기를 최소화하여 근접한 노드들의 정보를 최소화하고 또한, 스위치의 비정상적인 동작발생시 전원 재입력을 통한 캐시의 reflash 등의 방어기법을 사용한다. 이외의 방어 방법으로는 MAC address table을 Static 방식으로 변경하여 방어도 가능하다.

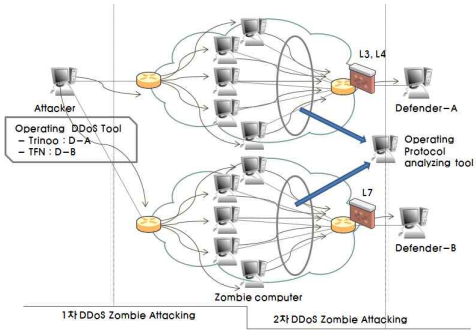
(2) ARP 공격 차단

ARP Spoofing 공격은 MAN In The Middle 공격기법을 이용하는 공격 형태로써 서로 다른 노드 사이에서 전송 정보를 변조하여 공격한다. 특정 노드가 가지고 있는 ARP 캐시의 Mapping 정보인 IP 또는 MAC address를 인용, 변조하여 공격자임을 숨기고 접근함으로써 원격 모니터링 등의 툴을 활용 정보를 유출하고 정보의 변조를 하는 공격이다. 따라서 가장 원시적이면서도 방어적인 측면서 가장 효과적인 방법은 각 노드가 가지게 되는 ARP 캐시의 정보를 주기적으로 리플래시 하는 방법이 가장 효과적이다. 또한, 캐시 사이즈를 최소화함으로써 근접 노드 정보 보유량을 줄이는 방법도 있다.

Ⅳ. TCP/IP Layer별 DDoS 공격에 대한 방어 실험

4.1 실험환경

Linux 기반의 Workstation급(Dual CPU, 2GB Memory, 500GB HDD, Gigabit NIC) CentOS를 서버로 20M급의 전용선 기반의 네트워크 인프라에서 구현하고 제2공격 시스템 및 제3공격 시스템을 구축하여, <그림 10>과 같은 실험환경에서 DDoS 공격 툴인 Trinoo를 이용해서 TCP/IP Layer의 각 단계별 Application, Transport, Internet, Network의 4계층에 대해서 대역폭 선점 Traffic 공격, 웹 Application Traffic 공격, Botnet 공격, Delete 공격을 시행하고, 또한, TFN 공격 툴을 이용해서 TCP/IP Layer 계층별 공격을 재시행 함으로써 공격대상에 따른 방어기법을 통해 최종 방어결과를 도출한다. 또한, 공중망의 상용 DDoS 공격 툴을 이용해서 TCP/IP Layer 계층별 공격도 시행한다. 이번 실험에서는 TCP/IP Layer의 Application 계층과 Transport 계층에 대한 DDoS 공격과 참고적으로 OSI 7 Layer의 7계층도 함께 실험한다. 또한, 계층별 운영 프로토콜에 대한 공격 상황 시 장애, 방어현황과 방어 상황 시 운영 프로토콜을 확인 및 분석을 위해 프로토콜 분석기를 운영 결과를 확인한다.



<그림 10> 실험환경

4.2 DDoS 기반의 취약점 공격

4.2.1 Traffic 공격

(1) 대역폭 선점 Traffic 공격

Transport 계층과 Network 계층의 전송 매개체인 Segment Datagram과 패킷을 비정상적인 흐름 형태로 끊김 없는 공격 형태로 구성하여, 최종 대량의 트래픽을 유발함으로써 가용 대역폭을 독점하는 형태로 공격을 시행한다. 지속적인 전송과 과부하가 계속 발생됨에 따라 인위적인 대량의 통신 Traffic을 발생된다. 따라서 정상적인 Network 계층의 패킷 흐름을 방해하고 제2, 제3의 Zombie를 발생시키는 공격을 Trino와 TFN 툴과 상용화된 과부하를 발생시키는 툴을 이용해서 공격을 시행한다. DDoS 공격의 프로세스에서 1차적인 공격에 해당된다.

(2) 웹 Application Traffic 공격

대역폭 선점 Traffic 공격의 경우는 Transport 계층과 Network 계층의 전송로를 대량의 전송 정보를 인위적으로 발생시킴으로써 전송로를 독점함으로써 장애를 발생시키는 반면 이번 공격은 단위시간 동안 특정 Host에 의하여 Unestablished Connection을 비정상적으로 증가시

켜 장애를 발생시키는 형태의 공격이다. 따라서 공격으로 인한 최종 장애 결과는 DDoS 공격의 프로세스에서 1차적인 공격과 동일한 결과를 나타낸다.

4.2.2 Botnet 공격

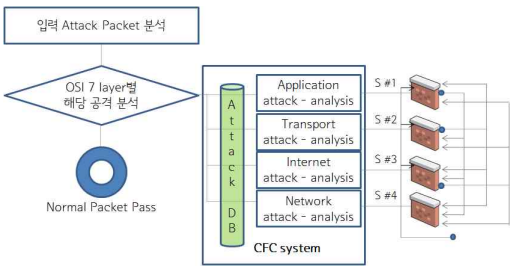
DDoS 공격의 프로세스에서 2차적인 공격 형태로써 원격 장애 유발과 같은 2차적인 Zombie를 의미하며, 자기 자신이 Zombie로써 특정 시스템에 대해 DDoS 공격을 발생시키는 Zombie임을 감지하지 못하도록 백그라운드화 되어진 DDoS 공격의 1차적인 피해자이자, 2차적인 공격자를 의미하는 공격이며, Trino와 TFN 툴 또는 특정 Botnet 툴을 이용해서 공격을 시행한다.

4.2.3 Delete 공격

인위적인 공격 프로세스인 DDoS 공격 프로세스에서 마지막 3차적인 공격 형태로써 공격으로 인한 장애와 공격 경로 등의 공격으로 발생되어진 모든 로그정보를 삭제함으로써 역추적 정보를 제거하는 최종 공격 형태로써 Zombie로부터 감염된 제2, 제3의 순차적인 Zombie의 공격을 유발하고 향후 IP 역추적 등의 역공격을 방해하기 위해 Zombie 시스템의 정보를 유출 또는 이전 DDoS 최초 공격의 정보 및 Zombie화 된 시스템의 기록을 삭제는 공격으로 본 실험에서는 Trino를 이용한 접근과 상용화된 백그라운드 정보 삭제 툴을 이용한다.

4.3 DDoS 공격에 대한 방어

DDoS 공격인 Traffic, Botnet, Delete 공격에 대한 방어를 위해 다중화 된 방화벽을 이용해서 TCP/IP Layer의 Application 계층으로부터 Internet 계층까지의 비정상적인 공격에 대해 본 방어를 위한 방법에서는 1차적으로 접근하는 비정상적인 공격을 TCP/IP Layer별 공격유형 분석을 통해서 공격자를 TCP/IP Layer별 공격의 형태분류에 따라 분리하고 2차적으로는 해당 TCP/IP Layer에 대한 보안정책을 설정한 방화벽으로 해당 공격을 유도하는 Forwarding 정책에 따라 <그림 11>과 같이 Filtering하는 Choose Firewall Channel [CFC] 시스템 모듈을 통해서 방어를 제어했다. Internal network과 External network의 단일경로를 통한 패킷의 전송라인을 구축하되 TCP/IP Layer별 각 계층에 준하는 공격성 패킷을 분석 및 각 계층에 대한 정책을 설정한 방화벽으로 패킷을 전송 하는 Channel 선택 모듈을 이용해서 각 계층별 DDoS 공격 탐지 및 방어한다[17 ,18 ,19].

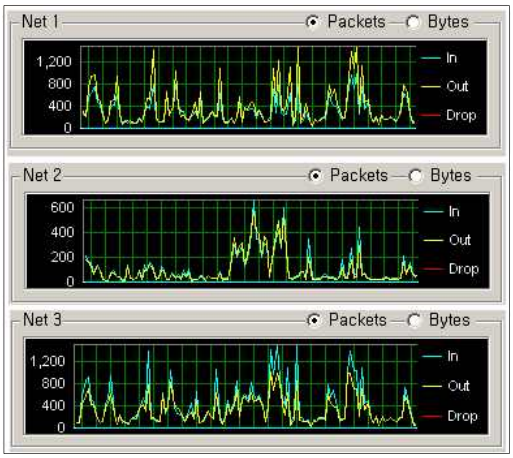


<그림 11> Choose Firewall Channel [CFC] 시스템 구성도

공중망에서 내부로의 접근 또는 공격성 접근이 이루어지는 형태는 매우 다양하고 집중화 되어 있다. 이러한 공격성 접근을 CFC 시스템은 특정한 네트워크 내에 공격유형별로 분리하여, 최초 유입되는 패킷을 TCP/IP Layer 상에 공격의 유형을 매칭 시켜 해당되는 정책을 설정한 방화벽으로 <그림 12>와 같이 전송되는 외부로부터의 유입 패킷을 CFC 시스템 모듈에 의해 방화벽을 선택 처리함으로써 In, Out, Drop 비율을 확인한다. 물론 패킷이 유입되는 경로가 중앙 집중화 되어 정책의 분리가 곧 네트워크의 성능을 오히려 저하하는 문제점을 제시할 수 있으나, 이는 최초 공격성 패킷 분석을 통한 가상 방화벽 선택 모듈로 정상적인 패킷의 경우는 CFC 시스템을 거치지 않고 내부로 유입되기 때문에 TCP/IP Layer별 방화벽의 병렬처리가 오히려 네트워크의 성능을 직렬처리에 비해 접속 Hit time이 1내지 2m/sec 빠른

네트워크 정보 전송의 향상을 보였다.

또한, CFC 시스템 공격 탐지와 방어기법의 가장 큰 특성과 기능은 TCP/IP Layer별 공격 형태를 분석하는 정책을 각각의 방화벽 단에 분산 적용함으로써 특정 공격에 대한 특화된 방어정책을 구성함으로써 내부 네트워크로 유입된 침입 Packet이 Broadcasting되어 침입의 범위가 확대되는 문제점을 제한하는 것이다.



<그림 12> 접속 히트 타임

4.4 DDoS 공격에 대한 결과 분석

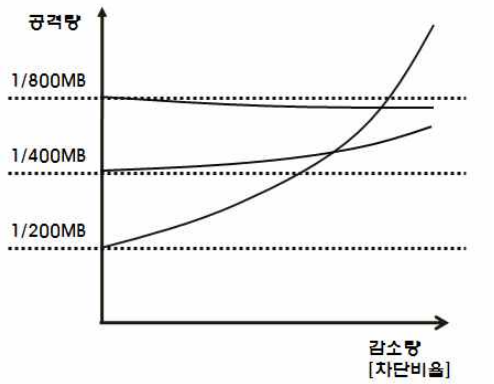
외부 접근 경로를 통해서 공격성 패킷이 유입되는 경우 1단계 해당 패킷이 TCP/IP Layer 구성 계층인 Application, Transport, Internet, Network 4단계 Layer 중 어느 TCP/IP Layer에 공격이 집중화 되어 있는지를 분석하고 2단계로는 해당 공격별 보안정책이 설정되어 있는 방화벽으로 패킷을 Forwarding하고, 정책에 의거 공격성 패킷이면, 패킷을 버리고 그 외의 정상적인 패킷이면, 패킷의 Source 목적지 IP address가 포함된 Area로 전송함으로써 한번의 패킷 분석과 한 번의 보안정책 적용으로 정상적인 패킷만을 선별적으로 받아들인다. CFC 시스템의 1단계 공격성 패킷 분석을 위한 TCP/IP Layer별 공격유형 분석을 위한 기본 형태는 TCP/IP Layer별 분류 및 정의하고 이를 CFC 시스템의 공격 패킷-DB화 한다. 최초 CFC 시스템의 패킷-DB는 공격성 패킷을 지속적으로 분석함에 따라 누적된 정보를 주기적으로 2단계의 정책에 반영하여, 보안정책을 적용한다. CFC 시스템의 2단계는 TCP/IP Layer별 공격을 1단계에서 분석하여, 공격의 성격을 정의함에 따라 해당 공격에 대한 정책을 탑재하고 운영 중인 방화벽으로 해당 공격성 패킷을 Forwarding한다. Application 보안정책은 Message 단위로 외부 접근 정보에 대한 정책을 설정하며, Message 해석을 통해 정상적인 접근인지를 확인 통과 또는 차단한다. 또한, Transport 보안정책은 Segment Datagram단위로 외부 접근 정보에 대한 정책을 설정하여, Segment Datagram해석을 통해 정상적인 접근인지를 확인 통과 또는 차단한다. 그리고 Internet 보안정책의 경우는 패킷 단위로 외부 접근 정보에 대한 정책을 설정하여, 패킷 해석을 통해 정상적인 접근인지를 확인 통과 또는 차단하며, Network 보안정책 역시 Frame단위로 외부 접근 정보에 대한 정책을 설정하여, Frame해석을 통해 정상적인 접근인지를 확인 통과 또는 차단한다. 7.7 DDoS 공격을 포함한 해커의 DDoS 공격에 대하여 실제 인터넷에서 TCP/IP Layer별로 공격대상을 분석하였다. 또한, Choose Firewall Channel [CFC] 시스템 모듈을 통해서 TCP/IP Layer별 정책을 분리하여, 정책을 병렬화한 결과공격 유형별 분석을 통한 학습형 데이터베이스가 누적되어 다양한 공격 형태를 사전에 분리 및 가상의 CFC 시스템을 통해서 방어기기로의 외부로부터 유입되는 침입을 직접 방어를 했다. 기존 운영하던 방화벽들을 CFC 시스템으로 구현 침입정보를 가진 이질적인 데이터베이스를 특정 형태로 일원화하고 실시간으로 각 단계별 방어정책마다 동일한 데이터베이스를 활용함으로써 물리적인 특성이 다소 상이한 장비들로 구현이 가능하다는 장점이 있다. 이는 특정 TCP/IP Layer에 해당 되는 공격에 대한 1:1 정책이 이루어지므로 호환성이 없는 경우의 네트워크간의 방화벽에서도 본 CFC 시스템 적용이 가능하다. <표 3>과 같은 제안된 네트워크별 처리 TCP/IP

Layer와 해당 TCP/IP Layer에 준하는 공격들을 명시하고 운영정책을 명시하고 있다. 이처럼 공격에 대한 분석 단계가 정확하게 TCP/IP Layer별로 공격 목적을 인지한다면, 보안 취약성을 최소화하고 공격성 접근이 차단된다.

<표 3> CFC 접근 공격과 정책영역과 순위

구분	Policy Area	Policy Sequence	Attack
Segment 1	L1 ~ L2	4	MAC Flooding, MAC 변조, ARP 공격
Segment 2	L3	3	IP 변조, DHCP 공격, ICMP 공격
Segment 3	L4	2	TCP Syn Flooding, UDP Flooding 등

또한, CFC시스템을 적용함으로써 TCP/IP Layer 계층별 공격형태 분류에 따른 침해 감소량을 <그림 13>와 같이 확인할 수 있다.



<그림 13> 계층별 정책비율 설정에 따른 각 단계별 공격 평균비율 상승에 따른 침해차단 비율[감소량]

Ⅴ. 결론

본 논문에서는 다양한 DDoS 공격을 1차적으로 TCP/IP Layer별 공격으로 분리하고 2차적으로는 해당 TCP/IP Layer에 대한 DDoS 공격. 즉, TCP/IP Layer별 공격을 방어할 수 있는 방화벽 다중화 정책을 통해서 DDoS 공격을 방어했다. 또한, CFC 시스템을 통해 보다 세부적으로 네트워크를 분할하는 방어 전략으로 네트워크를 세그먼트 단위로 분할하고 TCP/IP Layer별 공격의 형태를 분리 정책을 적용함으로써 정책과 로드의 반비례를 해소함에 따라 적절한 보안정책을 적용시킬 수 있고 Segment별 분산대응으로 관리 시스템 정책의 분업화를 통해 최초 패킷 유입을 담당하는 방화벽의 문제점을 해소하는 분할보안 관리 시스템 CFC 모델을 적용하였다. 또한, CFC 시스템의 TCP/IP Layer별 공격에 대한 데이터베이스를 지속적으로 학습하고 TCP/IP Layer별 데이터베이스를 공격에 따른 query로 구성하는 등의 다양한 학습지속형 CFC 모듈을 개발해야 한다. 향후 연구방향으로는 CFC를 구현하기 위한 단위 세그먼트 당 방화벽 시스템 구현이라는 Cost 부문의 과도한 하드웨어 도입 문제점이 있어 이를 CFC 시스템으로 하여금 세그먼트까지 가상으로 구현하는 확장된 연구와 대응모델에 대한 연구가 필요하다.

참고문헌

[1] 연합뉴스, http://www.yonhapnews.co.kr, “DDoS 악성코드 유포 개요,” 박영석, 2009.7.27.

[2] 시스코코리아, DDoS 공격 비상, 어떻게 대처할 것인가?, 2009.7.16.

[3] 한국인터넷진흥원, http://www.kisa.or.kr/jsp/notice/press_detail.jsp, 분산 서비스 거부공격(DDoS)으로 인한 국내 주요 홈페이지 인터넷 접속 장애, 이용자보호팀 신화수, 2009.7.8.

[4] 전용희, 장종수, 오진, “DDoS 공격 및 대응 기법 분류,” 한국정보보호학회논문지, 제19권, 제3호, 2009, pp. 46-57.

[5] Hunt, R, “Internet/Intranet firewall security-policy, architecture and transaction services,” Computer communications, Vol.21,

No.13, 1998, pp.1107-1123.

[6] Liu, A. X., Gouda, M. G, "Firewall Policy Queries," Vol.20, No.6, 2000, pp.766-777.

[7] 노시춘, "네트워크보안 인프라의 차단구조 설계방법," 디지털산업정보학회논문지, 제2권, 제2호, 2006, pp.10-20.

[8] 천재홍, 박대우, "VoIP의 DoS공격 차단을 위한 IPS의 동적 업데이트엔진," 한국컴퓨터정보학회논문지, 제11권, 제6호, 2006, pp.165-174.

[9] Schultz, E. E, "When Firewalls Fail: Lessons Learned From Firewall Testing," Network security, 1997, pp.8-12.

[10] 천우성, 박대우, "DoS공격에 대한 N-IDS 탐지 및 패킷 분석 연구," 한국컴퓨터정보학회논문지, 제13권, 제6호, 2008, pp.217-224.

[11] 이창우, 김석훈, 송정길, "분산환경에서의 침입방지를 위한 통합보안 관리 시스템 설계," 한국컴퓨터정보학회논문지, 제10권, 제1호, 2006, pp.75-82.

[12] Wool, A, "The use and usability of direction-based filtering in firewalls," Computers & security, Vol.23, No.6, 2004, pp.459-468.

[13] Liu, A. X, "Firewall policy verification and troubleshooting," Computer networks, Vol.53, No.16, 2009, pp.2800-2809.

[14] Pozo, S, Ceballos, R, Gasca, R. M, "Model-Based Development of firewall rule sets: Diagnosing model inconsistencies," Information and software technology, Vol.51, No.5, 2009, pp.894-915.

[15] 박원형, 국윤주, 이수연, "SNS를 이용한 분산서비스 거부(DDoS) 공격 분석 및 탐지 방안 연구," 정보보안논문지, 제9권, 제1호, 2009, pp.151-159.

[16] 이인희, 박대우, "IP 역추적 설계 및 보안감사 자료 생성에 관한 연구," 한국컴퓨터정보학회지, 제15권, 제1호, 2007, pp.53-64.

[17] 전정훈, 전상훈, "효율적인 네트워크 보안운영을 위한 Exclusive Firewall 관한 연구," 한국컴퓨터정보학회논문지, 제12권, 제2호, 2007, pp.93-102.

[18] 김선호, 윤명철, 노병희, "고속 인터넷 백본망에서의 분산형 서비스 거부 공격 탐지 방법," 한국통신학회논문지, 제32권, 제2B호, 2007, pp.90-99.

[19] 이영교, 박종순, "정부 주요기관에 대한 사이버 공격의 대처 방법", 디지털산업정보학회논문지, 제4권, 제2호, 2008, pp.39-47.

■ 저자소개 ■

서 우 석
Seo, Woo Seok

2006 숭실대학교 정보과학대학원 정보통신융합학과(공학석사)
2009~현재 숭실대학교 일반대학원 컴퓨터학과 (박사과정)

관심분야 : 정보보호, 네트워크 보안, 방화벽, Router & Network Design 등
E-mail : sswss2003@yahoo.co.kr

박 대 우
Park, Dea Woo

1998 숭실대학교 컴퓨터학과(공학석사)
2004 숭실대학교 컴퓨터학과 (공학박사)
2000 매직캐슬정보통신 연구소 소장, 부사장
2004 숭실대학원 정보과학대학원 정보보안학과 겸임조교수
2006 정보보호진흥원(KISA) 선임연구원
2007~현재 호서대학교 벤처전문대학원 조교수

관심분야 : 정보보호, 유비쿼터스 네트워크 및 보안, 보안 시스템, CERT/CC, Forensic, VoIP 보안, 이동통신 및 WiBro 보안, IT-Convergence
E-mail : prpf1@paran.com

전 문 석
Jun, Moon Seog

1981. 2 숭실대학교 전자계산학과 졸업
1986. 2 University of Maryland Computer cience 석사
1989. 2 University of Maryland Computer Science 박사
1986. 9~1989. 12 University of Mary 강사
1989. 3~7 Morgan State University 조교수
1989. 9~1991. 2 New Mexico State University Physical Science Lab. 책임연구원
1991. 3~현재 숭실대학교 정교수

관심분야 : 정보보호, 네트워크 보안, 전자여권, 암호학
E-mail : mjun@ssu.ac.kr

논문접수일 : 2010년 9월 20일
수 정 일 : 2010년 10월 20일
게재확정일 : 2010년 10월 25일