韓國 컴퓨터情報學會 2006동계학술발표논문집&학회지
第14卷 第2號, 2006. 12.

VoIP의 DoS공격 차단을 위한 IPS의 동적 업데이트엔진

천 재 홍*, 박 대 우*

A Dynamic Update Engine of IPS for a DoS Attack Prevention of VoIP

Jae Hong Cheon*, Dea-Woo Park*

요 약

본 논문은 VoIP 서비스 네트워크에서 UDP, ICMP, Echo, TCP Syn 패킷 등을 조작한 SYN Flooding 방법, TCP/UDP을 이용한 어플리케이션을 통한 DoS 공격, IP Source Address Spoofing과 Smurf을 이용한 공격, 웜과 트로이목마를 혼합한 알려지지 않는 DoS 공격을 하였다. IPS에서 방어를 위한 동적 업데이트 엔진의 필요성을 정의하고, 엔진의 설계 시에 내·외부의 RT통계에서 트래픽 양을 측정하며, 학습모듈과 통계적 공격에 대한 퍼지 로직 엔진 모듈을 설계한다. 엔진은 3가지 공격 등급(Attack, Suspicious, Normal)을 판단하여, Footprint Lookup 모듈에서 AND나 OR 연산을 통해 최적의 필터링 엔진 상태를 유지한다. 실험을 통해 IPS 차단 모듈과 필터링엔진의 실시간 업데이트되어 DoS 공격의 차단이 수행됨을 확인하였다. 실시간 동적으로 업데이트되는 엔진과 필터는 DoS 공격으로부터 VoIP 서비스를 보호하여 유비쿼터스 보안성을 강화시킨 것으로 판명되어졌다.

Abstract

This paper attacked the unknown DoS which mixed a DoS attack, Worm and the Trojan horse which used IP Source Address Spoofing and Smurf through the SYN Flooding way that UDP, ICMP, Echo, TCP Syn packet operated, the applications that used TCP/UDP in VoIP service networks. Define necessity of a Dynamic Update Engine for a prevention, and measure Miss traffic at RT statistics of inbound and outbound parts in case of designs of an engine at IPS regarding an Self-learning module and a statistical attack spread, and design a logic engine module. Three engines judge attack grades (Attack, Suspicious, Normal), and keep the most suitable filtering engine state through AND or OR algorithms at Footprint Lookup modules. A Real-Time Dynamic Engine and Filter updated protected VoIP service from DoS attacks, and strengthened Ubiquitous Security anger, and were turned out to be.

▸ Keyword : DoS Attack, Dynamic Update Engine, IPS, Ubiquitous Security, VoIP

• 제1저자 : 천재홍, 교신저자 : 박대우(prof1@paran.com)
* 숭실대학교 정보과학대학원 정보보안학과

Ⅰ. 서 론

컴퓨터와 통신이 합쳐지는 BcN(Broadband Convergence Network)에서의 IPv6와 USN(Ubiquitous Sensor Network)를 통해서 유비쿼터스 사회(Ubiquitous Society)로의 전환이 급속히 이루어지고 있다. 이에 따라 업무도 인터넷을 통한 업무로의 전환이 급속하게 이루어지고 있다. 특히 음성서비스는 업무를 추진하고 처리하는 과정에서 확인과 의견 교환을 하는 중요한 수단이다. 지금까지 유선상에서 업무 전달은 기존 PSTN(Public Switched Telephone Network)에 의존하고 있다.

PSTN의 음성서비스를 인터넷의 IP을 사용하여 그림 1.과 같이 음성을 전송하는 기술을 VoIP(Voice over Internet Protocol)라고 한다. VoIP 기술을 기반으로 제공되는 서비스는 인터넷전화 서비스 또는 인터넷 텔레포니(Internet Telephony)로 부르고 있다. VoIP 서비스는 인터넷 콜센터, 다자간 화상전화 서비스, 사용자 위치정보 제공 등 다양한 애플리케이션 개발 등 다양한 응용이 가능하므로 경제성을 가진 비즈니스 모델로 가능성이 크다고 할 수 있다.

하지만 VoIP 서비스는 PSTN에 비해 열악한 통화품질과, 착신통화의 어려움, 중요 정보의 노출 및 인터넷의 취약점 공격에 따른 문제점 등으로 인하여 활용에 있어 적극적인 투자가 이루어지지 않았다. 그러나 정부의 IT839 정책에 8대 신규 서비스에 포함됨에 따라 VoIP 기술을 통한 PSTN과 인터넷망, 무선통신망을 연동하는 음성 및 영상 멀티미디어 서비스가 광대역 통합망의 핵심 기술로 떠오르면서 점차 상용화가 확대되고 있다.

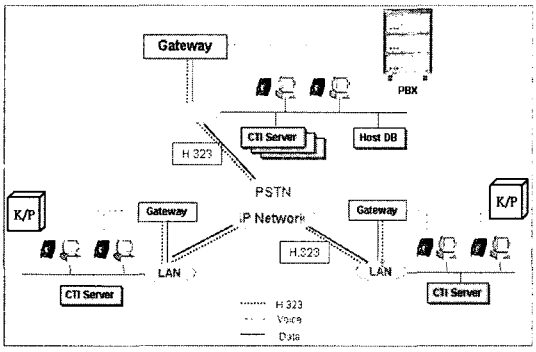

그림 1. VoIP 서비스 망
Fig. 1 VoIP Service Network

현재의 VoIP 서비스는 인터넷 네트워크에 연결된 노트북이나 PC에서의 프로그램 형태의 소프트폰 형태이거나, 기존의 전화기와 유사한 인터넷전화 형태, 그리고 와이브로(WiBro)와 연계된 무선단말의 VoIP 서비스가 있다.

VoIP 서비스는 기존의 인터넷 망을 그대로 활용함에 따라 개방형 인터넷 망에서 발생할 수 있는 보안 취약성이 그대로 존재한다[1]. VoIP 시스템 고유의 취약성을 이용한 공격에 대해서 방화벽(Firewall)으로만 방어하기는 어렵다[2]. 따라서 기존의 PSTN과 유·무선 인터넷 망의 연동에 따른 기존과 다른 새로운 취약점의 발생하게 된다[3]. VoIP 보안 위협으로는 도청과 스니핑 및 서비스 거부(DoS) 공격, 음성 스팸 등이 있다[4].

그림 2.에서 VoIP 서비스에서 DoS 공격은 일반적으로 전체 인터넷 서비스를 방해하거나 특정 VoIP 음성 서비스가 동작하지 않거나, 네트워크 접속 및 서비스 등이 일시적으로 제 기능을 발휘하지 못하게 하는 것이다. 보안회사인 시만텍은 2006년 10대 보안 위협의 하나로 'VoIP 위협 증가'를 꼽았다[5]. 최악의 공격 시나리오의 경우 수백만 명이 접속하는 인터넷 전화의 동작이 멈추는 경우도 예측할 수 있다.

VoIP 서비스의 제공에 따라 VoIP의 취약점 공격에 대한 취약점 분석과 함께, 엔진과 필터링 엔진에 대한 실시간으로 동적인 업데이트가 필수적이다. 특히 새로운 공격 패턴에 대해 제로 데이 공격(Zero-Day Attack)[6]에 대해 적절한 대응을 할 수 없다.

인터넷에서 DoS공격을 방어하는 방어 시스템으로 IPS(Intrusion Prevention System)가 사용되고 있다.

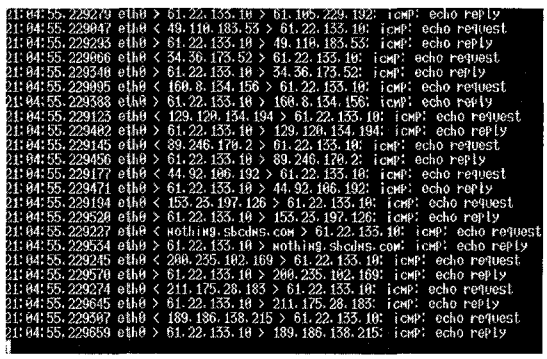

그림 2. DoS 공격 화면
Fig. 2 DoS Attack

IPS에서의 IDS가 가지고 있는 시그니처(Signature) 기반에다가 유해 트래픽을 차단할 수 있는 통계적 방법(Anomaly Detection)을 사용하여 DoS 공격을 차단 할

수 있다.

IPS에서 DoS 공격을 차단하기 위해 호스트 격리(Host Quarantine), 스트링 매칭, 연결 쓰로팅(Connection Trotting), 어얼리버드(Earybird) 시스템 등이 있다[7].

이 외에도 IPS에서 DoS 공격을 늦추고 분리시키기 위한 방법으로 합법적인 애플리케이션의 지속적인 운영은 허용하면서 웜 트래픽의 외부 확산을 줄이는 방법이 있다.

IPS에서 DoS 공격을 실시간으로 차단하고, IPS 방어 시스템들이 효율으로 작동하기 위해서는, 탐지와 차단에 대한 실시간 업데이트(Realtime Up-data) 엔진이 필수적이다[8]. 탐지와 차단에 대한 실시간 업데이트 엔진이 효율적으로 작동하느냐에 따라 IPS의 보안에 대한 효율성과 보안성능이 결정될 것이다.

따라서 본 논문에서는 VoIP용 ISP시스템을 이용 DoS에 대한 공격을 탐지하고 이를 즉각적으로 차단할 수 있는 동적 실시간 동적 업데이트 엔진(Dynamic Update Engine)의 필요성능 정의하고, 엔진을 설계하며, DoS 공격 통한 실험을 통해 효과에 대해 연구를 함으로써 VoIP 서비스의 안정적으로 운영 환경과 VoIP 보안을 통한 유비쿼터스 보안을 강화시키는 정보보호의 사회적 기반을 마련하는데 의의가 있다.

II. 관련 연구

VoIP 서비스의 취약점과 해커가 공격할 수 있는 취약내용에 대한 DoS공격 기술과 DoS공격 유형, 해커가 공격을 할 때 사용하는 공격 툴, 그리고 IPS의 방어기술 및 실시간 업데이트 엔진에 관하여 관련연구를 한다.

2.1. VoIP 서비스의 취약점

최근까지 알려진 VoIP 관련 보안 취약성[9]은 표 1.과 같이 요약할 수 있다. 시스템 정보와 IP 주소가 쉽게 노출될 수 있는 프로토콜 취약점이 다수 보고되었다.

2.2. DoS 공격

DoS 공격은 멀티태스킹을 지원하는 운영체제에서 발생할 수 있는 공격 방법으로서, 해커가 감염시킨 공격자들의 컴퓨터와 네트워크를 이용하여, 공격대상의 시스템의 리소스를 독점(Hogging)하거나, 시스템의 가용성을 소진시켜 대상 시스템이 다른 사용자들에게 올바른 서비스를 제공하지 못하게 만드는 것을 말한다.

표 1. VoIP DoS 취약점과 취약 내용
Table. 1 DoS Vulnerability point & contents of VoIP

CVE No.	VoIP 서비스의 취약점 대상 과 취약 내용
CVE-2006-1973	Linksys RT31P2 라우터는 비정형화된 SIP메시지를 이용한 원격 DoS공격을 허용한다.
CVE-2006-0360	MPM SIP HP-180W Wireless IP 폰(WE00.17)은 원격의 공격자가 중요한 정보를 얻는 것을 허용하고 UDP 포트 9090을 사용한 DoS공격을 할 수 있다.
CVE-2005-3989	Avaya TN2602AP IP Media Resource 320 circuit pack before vintage 9 펌웨어는 원격의 공격자가 VoIP 패킷을 이용한 DoS 공격을 허용한다.
CVE-2005-3804	Cisco IP Phone (VoIP) 7920 1.0(8)전화는 UDP 포트17185로 VxWorks 디버거를 지원하며 원거리 공격자가 중요한 DoS공격을 하며 중요한 정보를 가져갈 수있게 해준다
CVE-2005-3803	Zyxel P2000W 버전 1 VOIP WIFI 폰 Wj.00.10은 DNS Server의 IP주소를 하드코딩 한다. 이것은 원격의 공격자가 DoS 공격을 할 수 있도록 허용하거나 Zyxel 폰의 세션을 가로채거나, 하드코딩된 DNS Server 주소를 숨길 수 있도록 해준다.
CVE-2005-3725	Zyxel P2000W 버전 1 VOIP WIFI 폰 Wj.00.-UDP 포트 9090을 이용하여 중요 정보 획득
CVE-2005-3724	Zyxel P2000W 버전 1 VOIP WIFI 폰 Wj.00.10은 원격의 공격자가 UDP 포트 9090을 이용하여 중요한 정보를 획득하거나 DoS 공격을 발생하도록 허용한다.
CVE-2005-3723	Hitachi IP 5000 전화 펌웨어1.5.6은 사용자가 SNMP 또는 TCP 포트 3390을 비 활성화 할 수 있도록 허용하지 않는다. 이것은 원격의 공격자가 CVE2005-3722를 이용하여 환경설정을 수정할 수 있게 해주거나 중요한 정보를 얻기 위해 Unidata Shell에 접근할 수 있게 하거나 DoS공격 발생을 하게 해준다.
CVE-2004-1977	3com NBX IP VOIP NetSet 환경설정 매니저는 원격의 공격자가 SafeChecks 모드에서 Nessus 스캔을 이용한 DoS 공격을 허용하게 한다.
CVE-2003-1114	Mediatrix Telecom VoIP 장치와 SIPv2.4와 SIPv4.3을 이용하는 게이트웨이 펌웨어는 원격의 공격자가 일으키는 DoS공격 또는 INVITE 메시지를 이용한 임의의 코드 실행을 허용한다.
CVE-2002-0835	PXE 서버는 원격의 공격자가 DHCP 패킷을 이용하여 일으키는 DoS 공격을 허용한다.

2.3. DoS 공격 유형

DoS 공격유형을 TCP/IP 구현의 버그를 악용한 공격, 2) TCP/IP 약점을 악용하는 SYN Flood, LAND Attack, 3) Smurf Attack같은 무차별적인 공격, 해커의 공격 툴 등[10]으로 관련연구를 한다.

1) TCP/IP 구현의 버그를 악용한 공격

- 죽음의 핑(Ping of Death) 공격

핑은 원래 최고 65535byte로 크기가 제한되어 있는데 이보다 큰 크기의 패킷을 송신하여, 시스템을 교착 상태에 빠뜨리거나 재시동 시킴으로써 서비스를 중지시킨다.

- Teardrop 공격

Teardrop은 IP 패킷이 전송과정이 잘게 나누어졌다가 다시 재조합하는 약점을 악용한 공격으로, IP 패킷은 하나의 큰 자료를 잘게 나누어서 보내게 되는데, 이때 offset을 이용하여 나누고, 도착지에서 offset을 이용해 재조합하게 된다. 이때 동일한 offset을 겹치게 만들어 시스템을 교착시키거나 충돌을 일으키거나 재 시동하게 만든다.

2) TCP/IP 약점을 악용하는 SYN Flood, LAND Attack

- SYN Flood 공격

SYN공격은 대상 시스템에 연속적인 SYN 패킷을 보내서 넘치게 만들어 버리는 공격으로, 각각의 패킷이 목적 시스템에 SYN-ACK 응답을 발생 시키는데, 시스템이 SYN-ACK에 따르는 ACK를 기다리는 동안, backlog 큐로 알려진 큐에 모든 SYN-ACK 응답들을 넣게 된다. SYN-ACK은 오직 ACK가 왔을 때나 내부의 비교적 길게 맞추어진 타이머의 시간이 넘었을 때만 이 3단계 교환 TCP 통신 규약을 끝내게 된다. 이 때, 공격자는 큐를 꽉 차게 만들어, 들어오는 모든 SYN 요구를 무시하고 시스템이 인증된 사용자들의 서비스를 할 수 없는 상황을 만든다.

- LAND Attack 공격

LAND 공격은 대상 시스템에 조작된 Source IP를 이용에 네트워크에 SYN 패킷을 넘치도록 한다. 이것이 호스트 컴퓨터가 자신에게 패킷을 보내 것처럼 보이게 되고 대상 시스템이 자기 자신에게 응답하기 전 까지 시스템은 올바르지 않게 작동되게 된다.

3) Smurf Attack같은 무차별적인 공격

- Brute-force 공격

Brute-force 공격의 예로 Smurf 공격이 있다. 대상 시스템의 IP 주소와 서브네트 마스크 등을 알게 되면, 해당 네트워크에 쓸모없는 대량의 데이터를 전송시켜 네트워크 용량을 초과시키고, 해당 네트워크의 라우터로 하여금 ICMP echo를 서브네트 안에 있는 모든 컴퓨터에 요구하게 된다. 이 결과 내부 네트워크에 많은 수의 호스트가 많은 양의 IMCP echo 요구 패킷을 생성하게 되고, 네트워크만 트래픽 폭주와 조작된 Source IP 주소에 병목 현상이 생기게 되어 결국 전체 대역폭을 전부 점유하여 통신을 못하게 한다.

- IP Spoofing 공격

호스트나 라우터로 하여금 해커의 패킷이 인증된 네트워크로 부터 온 것인 것처럼 IP를 Spoofing을 통해, 라우터나 방화벽에서 정상 패킷이 인증된 네트워크로 부터 전송된 것으로 의심 없이 통과 하도록 만든 다음 본인이 원하는 공격을 한다.

2.4. 해커의 공격 툴

해킹 툴에는 시스템의 취약점을 찾는 스캐너(Scanner), 패스워드 크래커(Password Cracker), 사용자의 키 값을 빼내는 키로거(Key Logger), 백오리피스와 같은 트로이목마 프로그램(Trojan Hacking Program), 공격 코드(Exploit Code) 등이 있다. 이러한 해킹 툴은 공격과 방어를 위한 보안취약점 진단에 사용되기도 한다.

2.5. IPS 방어

IPS(Intrusion Prevention System)는 침입방지시스템이며, 보안 측면에서 볼 때 침입에 대한 능동적인 대응(Active Response)을 하며, 방어의 실행 측면에서는 선처리 방어(Proactive Protecting) 기술을 이용한 동적 실행 보안 시스템이다. 능동 보안기술[11]은 침입에 대한 해당 트래픽의 근원지를 다양한 방법으로 입수, 근원적으로 차단해 제2, 제3의 침입을 막는데 중점을 둔다. 불법적인 공격이 침입하는 것을 실시간으로 탐지하여, 공격을 수행하는 커넥션을 끊거나, 프로그램 실행을 막아버림으로써 원천적으로 침입에 대한 방어 시스템이다.

2.6. IPS 실시간 업데이트 엔진

현재 IPS의 경우 고속 네트워크에서 하루 수백만 건의 로그 기록이 발생하는데, 네트워크 차원에서 이러한 데이터를 모두 수집해 분석하기는 매우 힘들기 때문에 IPS 시스템의 로그 축약 기술이 해결되지 않으면 안 된다.

또 해킹은 단순한 이벤트 보다는 연관성 있는 이벤트의 조합으로 이뤄지는 경우가 대부분이므로 연관성 분석은 필수이다. 실시간 패킷에서 네트워크를 위협하는 해커의 공격을 찾아내는 것은 어려운 일이다. 따라서 IPS 보안장치들이 자체 로그 데이터를 축약하는 기능이 개발되어야 하는 것이다. 이런 보안 요구에 따라 네트워크 트래픽 분석과 IPS의 보안 로그 분석을 통해 이상 징후를 실시간으로 인식하고, 인식된 이상징후에 대해 공격 패턴을 자동 추출하는 기술이 실시간 업데이트 엔진이다. 네트워크에서 웜 등의 공격을 바로 인식하고, 네트워크로 유입되는 트래픽을 제어할 수 있어야 한다.

III. VoIP에 대한 DoS 공격과 IPS 차단

3.1. VoIP 취약성에 대한 DoS 공격

VoIP 서비스에서 DoS 공격은 전체 인터넷 서비스를 방해하거나, 특정 VoIP 음성 서비스가 동작하지 않거나, 네트워크 접속 및 서비스 등이 일시적으로 제 기능을 발휘하지 못하게 하는 것이다. 안전한 VoIP 서비스는 기밀성·무결성·가용성 제공이 필수로 콜 성립·미디어 트래픽 전송 과정을 보호해야 한다[11].

VoIP 시스템에서 DoS 공격은 IP 시스템에 대한 가용성과 무결성 및 기밀성을 훼손하는 공격 방법 외에도, VoIP 서비스의 특성인 실시간 서비스 품질에 관한 시스템 고유의 취약성을 이용한 공격도 방어하기가 어렵다.

1) VoIP 가용성에 대한 DoS 공격

VoIP 망에 대한 가용성 침해 공격은 그림 3.과 같이 VoIP 서비스 망이 정상적으로 동작하지 못하도록 한다. 해커는 UDP, ICMP, Echo, TCP Syn 패킷 등을 조작하여 공격을 유발하며, 불필요한 패킷들을 공격 대상 시스템에 집중적으로 보냄으로써 시스템 자원의 가용성을 고갈시킨다.

VoIP 음성 서비스 중인 공격자가 TCP RST Brute force 공격을 할 경우 reset 명령에 의해 VoIP 서비스가 중단된다. 이처럼 초기에 호를 설정하는 과정과 호를 끊는 과정을 반복함으로써 시스템 자원을 고갈시키거나 소프트스위치에 비정상적인 요구를 과도하게 함으로써 정상적인 서비스에 방해를 유발시키는 공격방법이다.

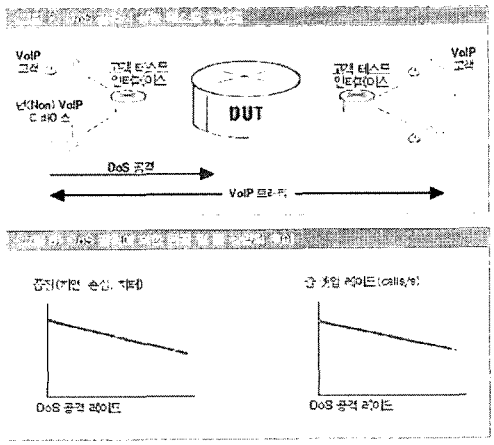

그림 3. DoS 공격 시 성능 테스트 구조
Fig. 3 Save a performance test in case of a DoS attack.

2) VoIP 무결성, 기밀성에 대한 DoS 공격

VoIP 인프라에 대한 무결성을 훼손하는 공격을 통해 VoIP 스팸 공격이나 위조된 통화시도(Spoofing Call), 변조된 RTP 삽입을 통한 음성통화 방해공격 등이 이용된다.

VoIP 인프라에 대한 기밀성 침해 공격으로는 음성 호나 음성 호를 위한 신호의 가로채기 등이 있다. 이러한 정보가 공격자에게 유출되면 음성통화자의 개인정보가 침해될 수 있으며, 이 정보를 이용한 해커의 공격에 이용될 수 있다.

3.2. DoS 공격에 대한 IPS 차단 메커니즘

VoIP의 DoS 공격에 대한 IPS의 방어를 전체적으로 표현하면 그림 4.와 같다. IPS의 차단기능에는 DoS 공격 차단을 위한 방어 메커니즘[12][13]을 포함한다.

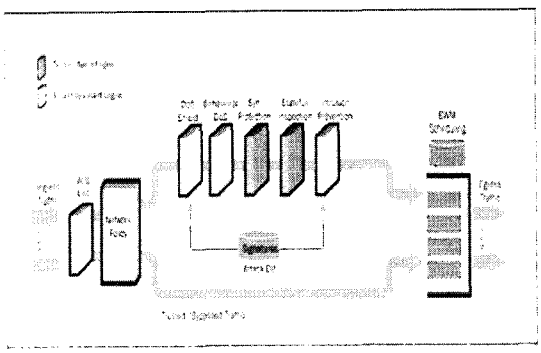

그림 4. DOS공격에 대한 필터링
Fig. 4 DoS Attack Filtering

1) Connection Limiting 메커니즘

ISP의 방어정책은 그림 5.처럼 DoS에 공격에 의한 TCP의 커넥션 수를 제한 한다. 즉 서버와 호스트에 과부하를 발생시키는 공격들에 대해 영향을 줄여서 내부의 가용성 자원을 보호할 수 있다.

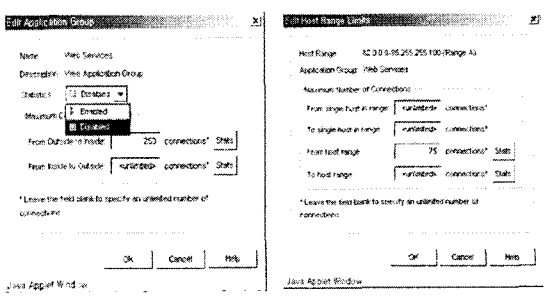

그림 5. 케넥션 제한
Fig. 5 Connection Limiting

2) SYN Flood 필터링 메커니즘

클라이언트로부터 VoIP 서버로 들어오는 오는 세션들 중 그림 6.처럼 SYN Flooding이 임계치(threshold)를 초과하여 TCP 핸드 쉐이킹이 맺어지지 않는 세션에 대해, 사전에 정의된 보안 정책에 따라서 위협 순위에 의해 IP 주소 값을 필터링 한다.

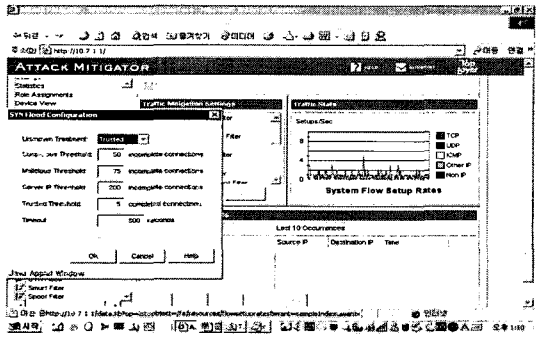

그림 6. SYN Flood 필터링
Fig. 6 SYN Flood Filtering

각각의 출발지 IP 주소는 [Unknown], [Trusted], [Suspicious], [Malicious]라는 위협 레벨 중 하나에 할당된다. 서버에서 열려있는 커넥션 수가 허용치를 초과하지 않는다면, [Unknown] 혹은 [Trusted] 중 하나인 주소 값으로 부터의 연결 시도는 목적지로 포워딩되어 진다. 의심스러운 단계인 [Suspicious]에 있는 주소 값으로 부터의 연결 시도는 설정 가능한 타임아웃 시간동안 블록킹 한다. 악의적인 단계 [Malicious]에 있는 주소 값으로 부터의 연결 시도는 바로 연결되지 않고, Attack Mitigator IPS에 의해 프록시화(proxied) 된다.

VoIP 서버들은 임계치에 의해 보호되고 만약 서버에 대해 열려져 있는 TCP 커넥션 수가 임계치를 초과하면, 이후 커넥션은 임계치가 초과해 있는 동안 프록시화(proxied)된다. 보안 설정에서 [Trusted] 단계를 유지 하도록 특정 호스트들을 설정할 수 있으며, 이 경우에는 이 호스트들에 대해서는 필터링 되지 않는다.

3) IP Source Address Spoof 필터링 메커니즘

그림 7.은 외부 네트워크로 부터 들어오는 패킷들 중 내부 네트워크에서 사용해야만 할 IP 주소 값을 가지고 들어오는 패킷들을 필터링하고, 내부 네트워크로부터 장비에 들어오는 패킷들 중 정의된 내부 네트워크의 주소가 아닌 패킷들을 필터링하여 차단한다. 내부 네트워크에서 사용 중인 IP 서브넷과 외부 라우터 인터페이스의 IP 주소 값들을 정의(Edge Device)하고 정의된 IP 서브넷들은 IP Source Address Spoofing 뿐만 아니라 Smurf 및 Fraggle 공격의 방어를 위해서도 사용할 수 있다.

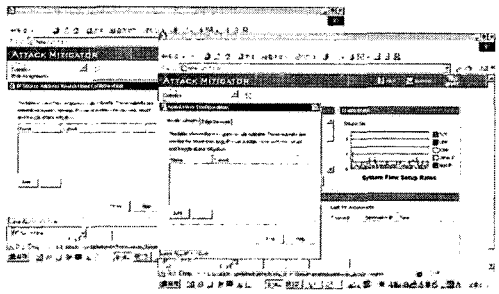

그림 7. IP Source Address Spoof 필터링
Fig. 7 IP Source Address Spoof Filtering

4) Nimda/Code red I, II 필터링 메커니즘

HTTP URI 값이 특정한 사용자에 정의된 시그니처에 해당되는 HTTP 트래픽을 필터링한다. 그림 8.에서 웜바이러스를 통한 기존 시그니처 편집 및 사용자 정의가 가능하며 화면의 우측하단에서 공격 시그니처의 이름, 분류, URI의 문자열 위치나 Wildcard의 사용으로 특정위치의 시작, 중간, 끝 정보를 정의할 수 있다.

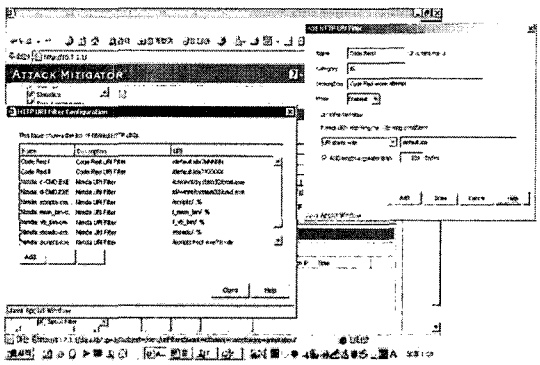

그림 8. Nimda/Code Red I, II 필터링
Fig. 8 Nimda/Code Red I, II Filtering

5) IP Address 필터링 메커니즘

출발지와 목적지의 IP 양쪽 모두가 정당하지 않은 주소를 가진 경우 그림 9.처럼 필터링한다. CIDR 표기법으로 하여 IP Address 범위로 지정하거나 있어, 출발지, 목적지 주소 또는 양쪽 모두의 주소를 필터링하여 차단한다.

이는 특정 출발지나 목적지 IP가 허용된 시간 동안 과도하게 들어올 경우, 특정 IP를 차단하는 기능이다.

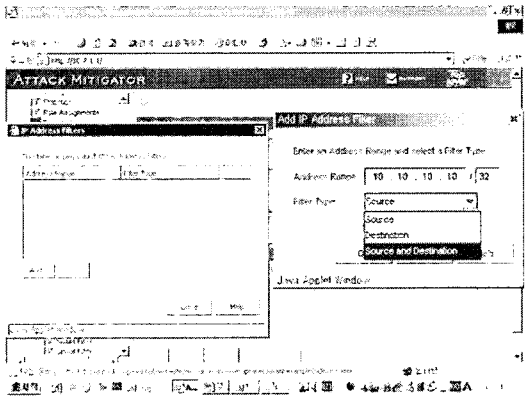

그림 9. IP Address 필터링
Fig. 9 IP Address Filtering

6) Application Rate Limiting 메커니즘

대역폭 제한 임계치값에 기반하여 내부 네트워크로부터 혹은 외부 네트워크에서 내부로의 어플리케이션 트래픽을 그림 10.처럼 필터링한다.

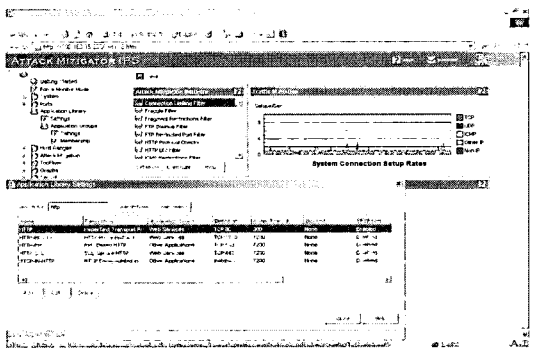

그림 10. 어플리케이션 대역폭 제한
Fig. 10 Application Rate Limiting

Application Libarary 안의 등록된 App list에서 특정 Application에 대한 Edit를 실행하여 외부와 내부 쪽 대역폭을 설정한다.

7) Application Blocking 메커니즘

TCP/UDP 포트 번호 기반으로 정의된 네트워크 어플리케이션을 그림 11.처럼 차단한다. 차단 목록에 등록된 Application Blocking list들에 대한 정보에서 블록킹 하고자 하는 Application의 외부와 내부의 방향성을 지정하여 추가한다.

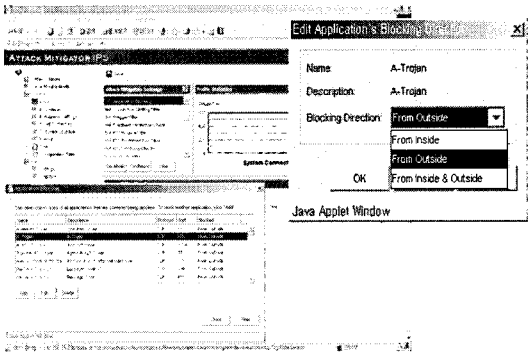

그림 11. 어플리케이션 블럭킹
Fig. 11 Application Blocking

8) 셀프-러닝(Self-learning) 차단 메커니즘

이 기능은 일정시간 동안 네트워크 트래픽을 모니터링하여, 특정 서비스의 트래픽을 학습한 후에 통계칠르 작성하고, 적정한 임계치를 넘어서는 트래픽은 차단하는 기능이다. 이 방법의 단점은 정상적이고 빈번한 사용자의 서비스까지 차단할 위험성을 내포하고 있다.

9) Offset Mask Pattern Condition 메커니즘

이 기능은 L3 ~ L4의 TCP/IP 헤더의 모든 정보를 이용한 필터링 차단 기능이다. 헤더의 토털 패킷 길이, 프로토콜 넘버, 시퀀스 넘버 등에 대해서 사용자 필터의 정의를 지원하는 기능이다.

10) Bandwidth Management 차단 메커니즘

이 기능은 각 서비스별로 우선순위 및 대역폭 설정을 통해 공격이 진행되는 상황에서도 필요한 서비스에 대해서는 대역폭만큼의 서비스를 보장해주는 기능이다.

IV. IPS 차단의 실시간 업데이트 엔진

4.1. IPS 차단 엔진의 실시간 업데이트 필요성

그림 12.처럼 VoIP에서의 DoS공격을 IPS에서 차단을 하고자 할 때 다양한 방법이 적용될 수 있다.

첫 번째는 가장 전통적인 차단 방법으로 시그니처를 이용한 차단 방법으로 IPS에서 공격차단을 위한 DB를 가지고 있으며 공격 발생 시 이와 매치되는 시그니처가 있는 경우 이를 차단하는 방법이다. 시그니처를 이용한 방법의 경우 엔진에 대한 실시간 DB 업데이트가 필요하다.

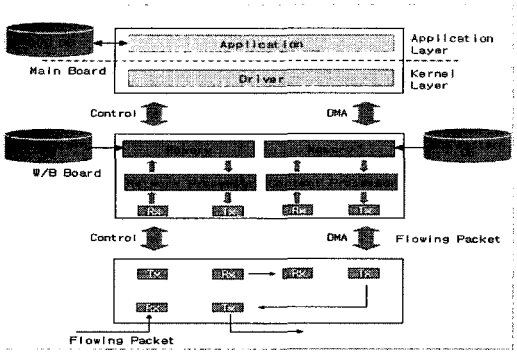

그림 12 IPS 방어 시스템의 업데이트 엔진.
Fig. 12 IPS Defense System Update Engine

두 번째는 임계치를 이용한 세션 수 제어 방법으로 특정 출발지 IP 혹은 목적지 IP가 IPS 엔진의 보안 정책에서 설정한 임계치를 초과해 유입되는 경우에, 임계치를 넘는 세션은 모두 차단하는 방법이다.

해당 방법은 사용자 환경에 따라서 임계치를 수동으로 설정해야 하며 특별한 이벤트 발생으로 인한 트래픽 증가 시 오탐이 발생할 수 있기 때문에 이러한 경우 관리자가 모니터링 모듈을 관리하여 적절한 임계치를 설정해야 한다.

하지만 관리자의 설정에는 한계가 있어 동적 업데이트 엔진의 효율성을 위해서는 Self-learning 모듈을 이용하여, 통계치의 자료를 DB화하여 나온 최적의 임계치에 대한 실시간 차단 메커니즘의 업데이트가 필요하다.

세 번째는 SYN-쿠키 혹은 SYN 프록시를 이용한 방법으로 사용자 간의 통신에서 IPS 장비가 프록시로 동작하면서 쓰리 핸드 쉐이크(Three Hand Shake)를 중간에서 대신하는 방법이다. 이때 사용자로부터 ACK 패킷에 대한 응답이 있는지를 검사하고 이에 대한 응답이 없으면 차단하는 방법이다. 이 경우에 ACK 패킷에 대한 응답 검증을 하여 차단할 것인지에 대한 실시간 동적 업데이트 엔진이 필요하다.

네 번째는 행위기반(Behavior) DoS 공격 발생시 IPS 필터링 룰 엔진에서 실시간으로 차단 룰을 만들고, 차단하는 방법이다. 이 경우 관리자는 필터링 룰에 관한 DB 업데이트나 룰 생성에 관한 실시간 동적 업데이트 엔진이 필요하다. 이와 같이 각각의 차단 방법 별로 특징을 가지고 있기 때문에 DoS 및 DDoS 공격 차단을 위해 이를 복합적으로 사용하게 된다면 VoIP를 보다 안전하게 보호할 수 있다.

4.2. IPS 차단 엔진의 실시간 업데이트 디자인

그림 13.에서 내부와 외부의 패킷은 RT통계(Real Time Statistics)를 통해서 들어오게 된다. 이곳에서 인바운드와 아웃바운드 트래픽 양을 측정하며, 측정과 연계된 Self-learning 모듈과 퍼지 로직 엔진(Fuzzy Logic Engine) 모듈로 트래픽을 보내게 된다.

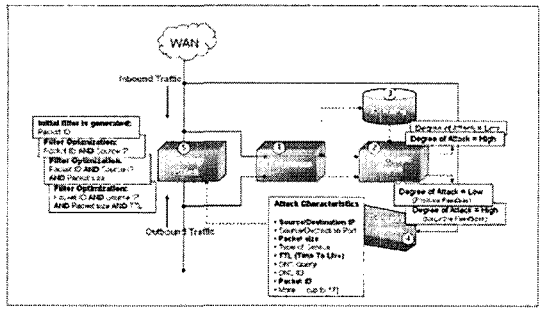

그림 13. 패킷의 RT 통계를 통한 트래픽 양을 측정
Fig. 13 Measure Miss traffic through RT statistics of a packet.

퍼지 로직 엔진 모듈은 통계적(Anomaly) 공격을 각 등급에 맞게끔 판단하는 엔진으로 DoS 공격의 등급을 3가지(Attack, Suspicious, Normal)로 판단한다. 또한 퍼지 로직 엔진 모듈은 계속적으로 Self-learning 모듈에 의해 업데이트됨으로써 최적화 상태를 유지하게 된다.

퍼지 로직 모듈에 의해 공격등급(Attack)으로 판정되었을 경우, 풋 프린트 룩업(Footprint Lookup) 모듈에서 AND나 OR 연산을 통해 최적의 필터를 자동으로 생성하도록 디자인 한다.

4.3. IPS 차단 엔진의 실시간 업데이트 실험

인터넷 네트워크에 연결된 구내 네트워크인 LAN 구간과 WAN 구간이 연결된 VoIP 네트워크에서 동적 업데이트엔진이 적용된 IPS를 설치하여 DoS 공격에 대한 공격 실험을 하였다. 공격은 UDP, ICMP, Echo, TCP Syn 패킷 등을 조작한 SYN Flooding 방법, TCP/UDP 포트 번호 기반으로 한 어플리케이션을 통한 DoS 공격, IP Source Address Spoofing과 Smurf을 이용한 공격, 웜과 트로이 목마를 혼합한 알려지지 않는 DoS 공격을 하였다.

1) 실험 환경 구성

❖ 공격자 시스템 사양

Linux RedHat 9.0(OS), Intel Pentium 2.66GHz (CPU), 448 RAM(Memory), 60GB(HDD)

❖ 공격 대상(Victim) 시스템 사양

Windows XP Professional(SP2) (OS), Intel Pentium 3.0GHz(CPU), 1024 RAM(Memory), 120GB(HDD)

❖ IPS 사양

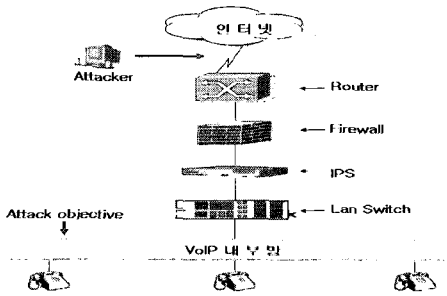

그림 14. Test Network 구성도
Fig. 14 A Test Network formation table.

Intel XeonMP 2.4GHz(CPU), 1024 RAM(Memory), 36GB(HDD), NIC 10/100 2개(관리용), Intel PRO 1000XF 4개 (차단용).

2) 시험 네트워크 구성도

그림 14.에 VoIP 서비스에 대한 DoS 공격의 실험을 위한 네트워크 구성도이다.

4.4. DoS공격에 대한 IPS 실시간 차단 실험

동적업데이트 엔진을 적용한 IPS를 네트워크에 적용했을 때 VoIP 서비스 네트워크에 대한 공격과 차단의 실험 결과는 그림 15.와 같다.

외부에서 해커가 다른 감염시스템을 이용하여 공격을 시도한 결과 그림 15.에서 ①에서 UDP, ICMP, Echo, TCP Syn 패킷 등을 조작한 SYN Flooding 방법 등으로 공격하여 DoS 공격을 유발한 첫 번째 공격은 성공적으로 차단됨을 보여 주고 있다.

그림 15.의 ②에서 TCP/UDP 포트 번호 기반으로 정의된 네트워크 어플리케이션을 통한 DoS 공격을 하였다. 셀프-러닝(Self-learning) 차단 모듈에서 공격을 탐지하고, 실시간 업데이트 엔진이 작동 되면서부터 필터링 모듈의 갱신에 의한 DoS 공격 트래픽은 차단되었다.

그림 15.에서 ③에서 IP Source Address Spoofing과 Smurf을 이용한 공격에서는 처음에는 정상적인 인증 패킷으로 인하여 공격에 따른 트래픽이 증가 하였으나, VoIP 서비스를 위한 트래픽의 임계치에 이르자 IPS의 방어 시스템에 의한 퍼지 로직 엔진 모듈이 DoS 공격의 등급을 공격(Attack)으로 판단하였다. 퍼지 로직 엔진 모듈은 계속적으로 Self-learning 모듈에 의해 업데이트하여 프린트 룩업 AND나 OR 연산을 통해 최적의 필터를 자동으로 생성하면서 공격의 차단이 실시간으로 이루어 졌다.

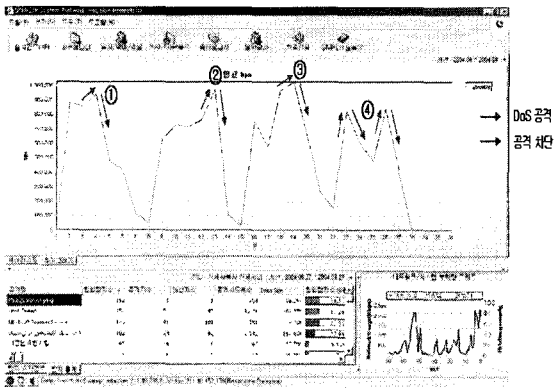

그림 15. DoS 공격에 대한 IPS 차단
Fig. 15 An IPS interception regarding a DoS attack.

그림 15.의 ④에서는 기존의 알려지지 않는 웜 바이러스와 트로이 목마를 침투시켜 정상적인 서비스를 가장한 폭주에 해당하는 알려지지 않는 DoS 공격을 실시하였다. 이 경우 Rate Limiting 메커니즘에 의해 L4 스위치가 트래픽을 분산시켰으며 계속되는 공격에 대하여, Bandwidth Management 차단 메커니즘과 Application Blocking 메커니즘이 작동하면서 퍼지 로직 엔진 모듈은 공격 IPdp 대한 트래픽을 실시간으로 차단하고 Self-learning 모듈에 의해 업데이트 엔진의 가동에 의해 필터링 룰이 갱신되면서 알려지지 않는 DoS 공격에 대한 네트워크 트래픽은 급속하게 감소하였다.

V. 결론

VoIP 서비스의 제공에 따라 VoIP의 취약점 공격에 대한 취약점 분석과 함께, 엔진과 필터링 엔진에 대한 실시간으로 동적인 업데이트가 필수적이다. 따라서 본 논문의 연구에서 연구되어진 동적 업데이트엔진을 구현한 IPS시스템은 VoIP시스템 가용성 보장하기 위해 내·외부의 트래픽 양을 지속적으로 측정하여 트래픽에 대해 분석하고, 이를 바탕으로 트래픽의 등급을 판단할 수 있는 필터를 각종 연산을 통해 자동으로 생성하여 업데이트하게 된다.

본 논문은 VoIP 서비스에 대한 DoS 공격으로 UDP, ICMP, Echo, TCP Syn 패킷 등을 조작한 SYN Flooding 방법, TCP/UDP을 이용한 어플리케이션을 통한 DoS 공격, IP Source Address Spoofing과 Smurf을 이용한 공격, 웜과 트로이목마를 혼합한 알려지지 않는 DoS 공격을 하였다.

IPS의 동적 업데이트 엔진에서 내·외부의 RT통계에서 트래픽 양을 측정하며, 학습모듈과 통계적 공격에 대한 퍼

지 로직 엔진모듈을 가동한다.

Self-learning 모듈에서 공격을 탐지하고, 실시간 업데이트 엔진이 작동하면서 Rate Limiting 메커니즘에 의해 L4 스위치가 트래픽을 분산시켰으며 계속되는 공격에 대하여, Bandwidth Management 차단 메커니즘과 Application Blocking 메커니즘이 작동하면서 퍼지 로직 엔진 모듈은 공격 IP에 대한 트래픽을 실시간으로 차단하였다. 엔진은 3가지 공격 등급(Attack, Suspicious, Normal)을 판단하여, Footprint Lookup 모듈에서 AND나 OR 연산을 통해 최적의 필터링 엔진 상태를 유지하였다.

향후 연구 되어야 할 과제로는, VoIP 서비스의 중요자원인 SBC나 Proxy Sever에서 SIP DoS공격이나, RTP Flooding 공격, DRDoS 공격 등을 이용하여, VoIP 서비스의 전체 네트워크가 마비되는 현상을 방지하기 위한, VoIP 서비스 사업자간의 공동 보안 대책에 관한 연구가 필요하다. 또한 DoS 공격에서도 패턴 암호화와 취약점을 이용한 해커의 새로운 공격에 대한 방어 전략도 연구 개발되어져야 할 것이다.

참고문헌

[1] NIST Draft. "Security Consideration for Voice over IP systems." April 2004.

[2] U.Roedig, R.Ackermann and R.steinmetz, "Evaluation and improving firewall for IP-telephony environment," Proc. of the 1st IP_Telephony Workshop (IPTel2000), April 2000.

[3] 구자현. "VoIP구현에서의 보안 고려사항." 한국인터넷기반진흥협회, 2005. 12.

[4] Thomas Poter etc, 7. "Practical VoIP Security," SYNGRESS. 2006.

[5] SYMANTEC. http://www.symantec.com. 2006.

[6] Georgios Portokalidis, Asia Slowinska, Herbert Bos. "Argos: an Emulator for Fingerprinting ZeroDay Attacks." EuroSys'06 ACM, pp18-21, April 2006.

[7] 능동형 침입차단시스템. NETWORK TIMES. 2006. 05.

[8] Deawoo Park. "A study about dynamic intelligent network security systems to decrease by malicious traffic". International Journal of Computer Science and Network Security, V.6, N.9B. pp 193-199. Sep 2006.

[9] Common Vulunability and Exposures. http://cve.mitre.org/cve/. 2006.11.

[10] 박대우, 서정만. "TCP/IP 공격에 대한 보안 방법 연구." 한국컴퓨터정보학회논문지, 제10권 제5호, pp217-226, 2005. 11. 30.

[11] 조영철. "SP 측면에서의 VoIP 보안 기술." NETWORK TIMES. 2005.11.

[12] DISA. IP Telephony & Voice over IP - Security Technical Implementation Guide ver2, Dec 2004.

[13] 박대우, 임승린. "해커의 공격에 대한 지능적 연계 침입방지시스템의 연구." 한국컴퓨터정보학회논문지, 제11권 제2호, pp44-50, 2006. 5. 31.

저 자 소 개

천 재 홍

2002년 8월 한국방송통신대학교 경영학과 (경영학사)

2006년 10월 숭실대학교 정보과학대학원 정보보안학과 (석사과정)

1997년 ~ 한국환경정책·평가연구원 환경정보센터 연구원 보안담당

관심분야 : 네트워크 보안, VoIP 보안, WEB 보안

박 대 우

1998년 숭실대학교 컴퓨터학과 졸업 (공학석사)

2004년 숭실대학교 컴퓨터학과 졸업 (공학박사)

2000년 매직캐슬정보통신 연구소 소장, 부사장

2004년 숭실대학원 정보과학대학원 정보보안학과 겸임조교수

2006년 정보보호진흥원 선임연구원

〈관심분야〉 유비쿼터스 보안, 네트워크 보안 시스템, VoIP 보안, 이동통신 및 WiBro 보안, Cyber Reality