퍼지 및 지능시스템학회 논문지 2003, Vol. 13, No. 2, pp. 148-153

서비스 거부 공격에서의 퍼지인식도를 이용한 네트워크기반의 지능적 침입 방지 모델에 관한 연구

A Study on Network based Intelligent Intrusion Prevention model by using Fuzzy Cognitive Maps on Denial of Service Attack

이세열* · 김용수* · 심귀보**

Se-Yul Lee , Yong-Soo Kim, and Kwee-Bo Sim

* 대전대학교 컴퓨터공학부

** 중앙대학교 전자전기공학부

요 약

서비스 거부 공격은 침입을 위한 침입시도 형태로 나타나며 대표적인 공격으로 Syn Flooding 공격이 있다. Syn Flooding 공격은 신뢰성 및 연결 지향적 전송서비스인 TCP의 종단간에 3-way handshake의 취약점을 이용한 공격이다. 본 논문에서는 네트워크 기반의 지능적 침입 방지 모델을 제안한다. 제안하는 모델은 Syn Flooding 공격을 탐지하기 위하여 패킷 정보를 수집하고 분석한다. 이 모델은 퍼지인식도(Fuzzy Cognitive Maps)를 적용한 결정모듈의 분석 결과를 활용하여 서비스 거부 공격의 위험도를 측정하고 공격에 대응하도록 대응모듈을 학습시킨다. 제안하는 모델은 Syn Flooding 공격의 위험을 격감 또는 방지하는 네트워크 기반의 지능적 침입 방지 모델이다.

Abstract

A DoS(Denial of Service) attack appears in the form of the intrusion attempt and Syn Flooding attack is a typical example. The Syn Flooding attack takes advantage of the weak point of 3-way handshake between the end-points of TCP which is the connection-oriented transmission service and has the reliability. This paper proposes a NIIP(Network based Intelligent Intrusion Prevention) model. This model captures and analyzes the packet informations for the detection of Syn Flooding attack. Using the result of analysis of decision module, the decision module, which utilizes FCM(Fuzzy Cognitive Maps), measures the degree of danger of the DoS and trains the response module to deal with attacks. This model is a network based intelligent intrusion prevention model that reduces or prevents the danger of Syn Flooding attack.

Key Words : 퍼지인식도, 침입방지시스템, 서비스 거부 공격, Syn Flooding Attack, Denial of Service

1. 서 론

네트워크 기술의 발달로 인하여 사회 모든 분야에 걸쳐 인터넷 환경이 널리 보급되었고, 인터넷의 품질서비스 향상 및 인터넷 사용료의 저렴화 등으로 인하여 일반인들도 쉽게 이용할 수 있게 되었다. 일반적인 인터넷 서비스의 특징인 정보 및 자원의 공유의 범위를 넘어서 e 비즈니스 등 여러 분야에도 폭넓게 이용되고 있는 실정이다. 그러나 이러한 인터넷의 확산은 긍정적인 측면도 있지만 부정적인 측면 또한 발생하게 되었다. 즉, 인터넷은 침입 의도를 지닌 일반인에게도 너무나 쉽게 침입에 대한 정보 및 관련 도구들을 제공한다는 것이다. 예를 들면, 해킹에 관련된 메일링 리스트, 뉴스그룹, 공개용 보안 프로그램 그리고 이와 관련된 보안 및 침입관련 문서 등이 이에 해당된다. 누구나 허가를 얻지 않은 상태에서 불특정 기관 및 단체에 침입하는 사례 또한 빈번히 일어나고 있다. 이러한 침입이 단순히 침입에 그치는 경우도 있으나 대부분 정보의 유출, 파괴 및 금융 사고와 같은 사회적, 경제적 손실이 심각한 지경에까지 이르고 있다. 이러한 침입 공격 중 침입을 위한 침입시도 과정으로 여겨지는 서비스 거부(Denial of Service : DoS)공격이 점차 늘어나고 있으며 2002년 현 시점에도 계속 발생하고 있다. 서비스 거부 공격이란 멀티태스킹을 지원하는 운영체제에서 발생할 수 있는 공격 방법으로서 구체적으로 한 사용자가 시스템의 리소스를 독점(hogging)하거나, 모두 사용해 버리거나, 파괴하여서 이 시스템이 다른 사용자들에게 올바른 서비스를 제공하지 못하게 하는 기술이다. 그러므로 시스템의 정상적인 수행에 문제를 야기 시키는 모든 행위를 서비스 거부 공격이라고 부르며 여기에는 매우 다양한 방법이 존재할 수 있다. 특히, 서비스 거부 공격은 고의적으로 발생할 수도 있지만 사용자의 의도와는 상관없이 실수로 발생 할 수도 있다. 서비스 거부 공격은 크게 주요 파일을 훼손시켜 목적 시스템의 동작을 방해하는 우회적 서비스 거부 공격과 목적 시스템의 자원 및 네트워크 데이터 전송을 위한 흐름제어 자원을 고갈시키는 공격으로 나눌 수 있다[1-7]. 최근 2-3년 동안에 발생한

접수일자 : 2002년 11월 15일
완료일자 : 2003년 2월 21일

Yahoo.com, Amazon.com 의 해킹사례가 서비스 거부 공격에 의한 대표적인 피해사례이다. 서비스 거부 공격의 가장 대표적인 공격방법으로는 Syn Flooding attack 이라 불리는 공격형태이다. Syn Flooding attack은 TCP 신뢰성 및 연결 지향적 전송서비스의 취약점을 이용하여 이루어지는데, 이러한 서비스 거부 공격은 인터넷 환경에서 가장 많이 사용되어지는 TCP 기반의 프로토콜 서비스를 지원하는 시스템에 크게 영향을 미치고 있다. 이 공격은 TCP 프로토콜자체의 구조적 결함을 이용하는데 이를 해결하기 위해서 여러 대안이 연구되어지고 있다.

지금까지 연구되어 온 방법으로는 Backlog Queue limit 와 Timeout value, Firewall, Semi-transparent gateway 등이다[1, 4, 8]. 첫 번째 Backlog Queue 방법은 Syn Flooding attack이 발생하면 Server에서는 연결요청을 수락하기 위하여 Syn RECEIVED가 발생한다. 이러한 요청이 지속적일 경우 Syn RECEIVED가 계속 발생하게 되고 Backlog Queue limit를 넘어서게 되어 서비스거부상태가 된다[4]. 이러한 점을 해결하기 위한 방법으로 Backlog Queue limit를 높이고 Syn RECEIVED의 수락시간(Timeout value)을 줄여주는 단순한 대응방법이 있다. 이 방법은 하드웨어(메모리)의 불필요한 낭비를 초래하므로 초기대응정책에 적합하나 근본적인 해결책은 되지 않는다. 두 번째 Firewall 경우에는 Client와 Server사이에 Firewall을 두고 항상 네트워크 흐름을 체크한다[8]. 그러나, Syn Flooding attack을 적절히 차단할 수 있다는 장점이 있으나 동시에 정상적인 네트워크 흐름에 대한 네트워크 지연율이 상당히 높다는 단점이 있다. 세 번째로 Schuba가 제안한 Semi-transparent gateway는 게이트웨이 또는 라우터에 Semi-transparent gateway를 두고 3-Way 핸드쉐이크 한다. 정상적인 SYN여부에 대해서만 ACK를 한다는 점에선 좋은 결과를 얻을 수 있었으나 이 역시 Semi-transparent gateway에서 처리로 인한 네트워크 연결 흐름 지연이 발생한다는 단점을 극복하지 못했다[8]. 이에 본 논문에서는 기존의 여러 대안에서 단점으로 지적된 네트워크연결 흐름 지연을 극복한 실시간 탐지 및 방지 모델을 제안한다.

본 논문에서는 제2장에서 서비스 거부 공격 중 Syn Flooding attack에 대해서 살펴보며 이를 해결하기 위한 방안을 알아본다. 제3장에서는 이러한 방안 중 TCP의 3-way Handshake 연결과정에서 발생하는 Half-Open 연결상태를 실시간으로 탐지하고 침입에 대한 위험도를 퍼지 인식도(Fuzzy Cognitive Maps : FCM)를 적용하여 침입여부를 판단하는 탐지모듈과 학습이 이루어지는 대응모듈을 추가한 침입탐지모델의 확장형태인 침입방지모델을 제안하고 테스트를 통한 성능을 알아보며 마지막장에서 향후 연구방향과 결론을 제시한다.

2. Denial of Service Attack

전형적인 침입유형 가운데 가장 보편화된 서비스거부공격은 멀티프로세싱을 지원하는 운영체제에서 발생할 수 있는 공격방법으로서 구체적으로 한 프로세서가 시스템의 자원을 독점하거나, 모두 사용해 버리거나 또는 파괴하여서 그 시스템이 다른 프로세서들에게 올바른 서비스를 제공하지 못하도록 하는 공격을 말한다. 그러므로 시스템의 정상적인 수행에 문제를 야기시키는 모든 행위들을 서비스 거부공격이라고 부를 수 있다. 서비스 거부공격의 특징으로는 루트권한을 획득하는 공격이 아니며, 데이터를 파괴, 변조 또는 훔쳐 가는 것을 목적으로 하는 공격이 아닌 점이다. 또한 공격의 원인이나 침입자를 추적하기 힘들며 다른 공격을 위한 사전 침입시도인 것이다. 이 공격유형의 방법은 다양하며 그 중 가장 대표적인 공격은 패킷 수준의 공격이다. 여기에 사용되는 종류는 ICMP, Finger, Syn Flood 등이 있다. 이 종류들의 유사점은 운영체제의 TCP/IP 모듈에 의해서 정상적으로 만들어져 보내지는 패킷들이 아니라 임의적인 조작에 의해서 만들어지거나 또는 서로 관련이 없는 패킷을 아주 작은 단위로 단편화(fragment)하여 이루어진다는 것이다. 본 연구에서는 이러한 패킷 수준의 공격 중 Syn Flooding attack에 대하여 다루고자 한다.

2.1 Syn Flooding Attack

TCP Syn Flooding 공격은 앞에서 거론되었듯이 TCP의 약점을 이용한 공격형태이다. 일반적으로 TCP는 신뢰성 및 연결 지향적 서비스이므로 서버와 클라이언트간에 연결 설정에는 그림 1과 같은 '3 way Handshake'라는 정상적 연결 흐름이 이루어진다.

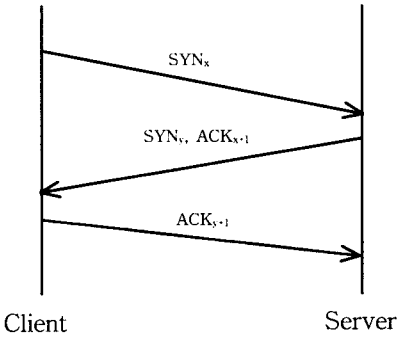


그림 1. 3-Way 핸드쉐이크
Fig. 1. Three-Way Handshake

여기서 클라이언트가 SYN_x를 요청하고 서버로부터 SYN_y와 ACK_{x+1}을 받은 후 ACK_{y+1}을 보내지 않으면 서버에서는 클라이언트로부터 응답이 올 것을 기대하고 반쯤 열린 'Half Open State'가 된다. 물론 얼마간 이런 상태가 유지된 후 다음 요청이 오지 않으면 해당 연결을 reset하게 된다. 이때 reset이 되기 전까지 메모리에는 backlog queue가 계속 쌓이게 되는데 이러한 reset이 되기 전에 지속적으로 이와 같은 요청이 아주 빠르게 이루어진다면 Syn Packet은 backlog queue에 쌓이게 되어 결국 메모리 용량을 넘어서게 되면 해당 포드에 대한 연결을 받아들일 수 없는 상태인 서비스 거부 상태가 된다[1-6].

2.2 Syn Flooding Attack 의 1차적 방어 대안

2.2.1 Backlog Queue 와 Half Open Time

실제 서비스 거부가 발생하는 원인으로 backlog queue에 더 이상 받아들일 수 있는 조건이 되지 않기 때문이다. 따라서, 원천적으로 해결방안이라고는 할 수 없지만 공격에 대하여 어느 정도 경감시킬 수 있는 해결방안으로써 backlog queue 크기를 증가시켜주는 것과 half open 상태의 대기시간을 줄이는 방법을 적용할 수 있다. 그러나 H/W 및 OS마다 서로 다른 메모리 용량과 backlog queue 크기가 할당되어 있어 정확한 크기증가 선정이 어려워진다. 다음은 리눅스

시스템에서 설정한 것을 예시한 것이다[3].

```
# cat/proc/sys/net/ipv4/tcp_keepalive_time-->7200
# cat/proc/sys/net/ipv4/tcp_keepalive_probes-->9
# cat/proc/sys/net/ipv4/tcp_max_ka_probes-->5
```

위와 같이 설정을 하고 지속적인 공격 테스트를 해 본 결과 공격이 이루어지는 순간동안 아주 짧은 순간이나마 시스템이 다운되는 현상이 주기적 반복형태를 띄고 있는 결과를 나타내었다. 그리하여 추가적인 해결을 위하여 다음과 같이 추가조치를 하였다. 바로, tcp_max_syn_backlog와 syncookies의 수치를 조절하는 것으로서 tcp_max_syn_backlog의 기본값인 256을 1280으로 설정하는 것이다.

```
/sbin/sysctl -w net.ipv4.tcp_max_syn_backlog=1280
```

이는 socket queue의 크기를 높여주는 방법인 것이다. 그러나, 이러한 대안은 지속적인 공격측면에서 볼 때 효율적이지 못하므로 적절한 대안이라 할 수 없지만 1차 방어측면에서 본다면 적절한 방어대안이라 할 수 있다.

2.2.2 Syncookies

syncookies에는 크게 Berkeley, Linux, Reset cookie가 있으며 '3-way handshake'에서 TCP 헤더의 Syn's sequence number, 소스 및 목적주소에 단방향 해쉬함수를 적용한 암호화 알고리즘을 이용한 방식으로 연결 설정이 정상적으로 이루어지지 않으면 더 이상 소스 경로를 따라 가지 않고 정상적 연결 요청에 대해서만 연결 설정을 하여 자원의 낭비를 줄이는 방법이다[2].

아래는 리눅스 시스템에서 공격 테스트를 위한 syncookies 설정 값으로써 공격시 시스템다운 현상을 어느 정도 차단하는 효과를 볼 수 있다.

```
/sbin/sysctl -w net.ipv4.tcp_syn_cookies=1
```

2.2.3 Packet Monitoring

라우터 및 게이트웨이를 통과한 후 시스템 접근에 앞서서 모니터링을 하는 방법으로써 들어오는 패킷을 잡아 분석하여 'half open state'를 요청하는 포트 및 IP address를 탐지하여 RST 등으로 연결 해제하는 방법이다. 본 논문에서는 제안하는 모니터링을 통한 탐지 또한 이 범주에 속한다.

이외에도 임의의 라우팅 테이블을 변경하여 트래픽이 전달되지 못하도록 ICMP redirects를 허용하지 않는 방법과 IP 소스 라우팅을 사용하여 목적지의 경로를 지정하여 믿을 수 있는 IP로 위장하지 못하도록 하는 소스 라우팅 패킷 허용 불능법 등이 있다[7, 8].

3. 탐지모델제안

3.1 탐지모델구조

본 논문에서 제안하는 탐지모델은 그림 2와 같이 여러 모듈 구조로 이루어져 있다. 전체적인 탐지모델구조는 들어오는 패킷을 이용하여 패킷을 분석하고 제어하는 모듈과 데이터저장, 그리고 'half open state'을 판단하는 판단모듈로 되어 있으며 추가로 대응모듈이 있다. 여기서 패킷캡쳐모듈은 그림 3과 같이 promiscuous mode에서 데이터링크층의 패킷을 캡쳐한 것이며 이를 프로토콜별 패킷을 받아서 세션별로 저장한다. 여기서 세션이란 Source IP와 Destination IP 그리고 프로토콜 종류가 같은 것들끼리 모아서 데이터저장 DB에 저장하는 동시에 패킷들을 판단 모듈로 보낸다. 패킷을 파싱(parsing)하여 로컬포트, IP address, Sequence number, 윈도우 크기 및 공격시간 등으로 저장시키고 패킷분석모듈을 통하여 syn패킷과 정상패킷으로 구분하여 1차 'half open state'를 탐지하게 된다. 여기서 탐지된 IP address는 퍼지인식도를 활용한 판단모듈을 통하여 블랙리스트 DB에 저장되고 시스템관리자에게 통보 하게된다. 이런 일련의 과정을 통하여 재차 공격 시에는 블랙리스트 DB와 각 패킷의 구성요소 비교알고리즘을 통하여 공격을 탐지하고 대응모듈을 가동하게 된다.

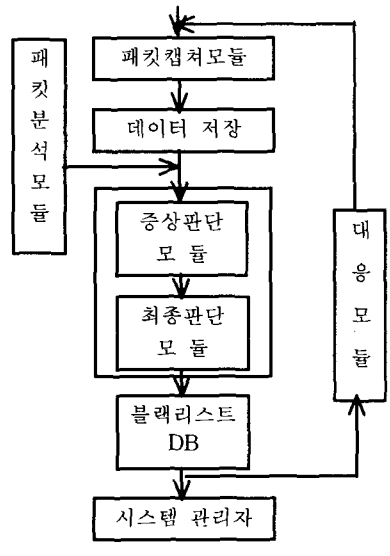


그림 2. 탐지 모델 구조
Fig. 2. Architecture of Detection Model

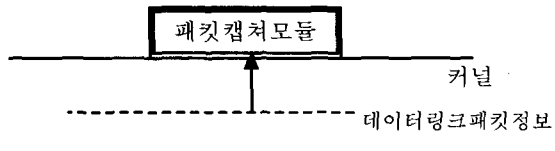


그림 3. 패킷 캡쳐 모듈
Fig. 3. Packet Capture Module

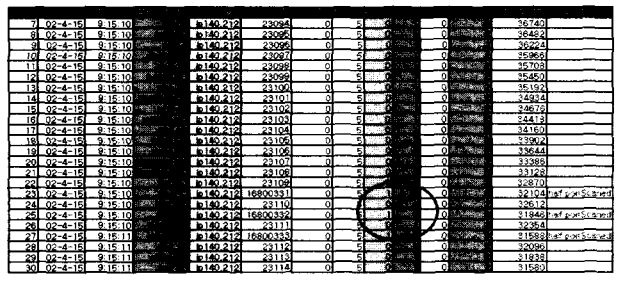
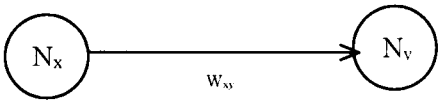


그림 4. 탐지로그항목
Fig. 4. Detection Log List

그림 4는 '데이터 저장' 에 저장된 탐지로그 항목이며 'SYN'과 'RST'의 수치가 각각 변경된 것과 해당 Sequence number 및 윈도우 크기가 변경된 것을 알 수 있는데, 이러한 항목들의 패턴을 감시하면 실시간으로 'half open state'를 탐지 할 수 있다.

3.2 판단모듈

판단 모듈은 퍼지 인식도(FCM)의 Causal knowledge reason을 이용하여 지능적 판단모듈구조를 설계하였다. FCM은 주어진 문제영역내의 각 개념들 사이에 존재하는 인과관계(Cause-effect relationship)를 나타내는 유향성 그래프(Directed graph)이다. 그림 5는 퍼지 인식도를 표현한 것으로써 각 노드와 노드사이의 가중치(링크)가 W_{xy}=0인 경우에는 각 노드사이에는 아무런 관련이 없는 것을 의미하며 $W_{xy}\neq 0$ 경우에는 그림 5와 같은 의미를 부여한다. 단순한 FCM에서는 인과관계 값을 {-1, 0, 1}로 취할 수 있다. 따라서 이경우의 인과관계는 최대 또는 최소의 정도로 발생한 것을 의미한다[9].



$W_{xy}>0$; N_x 수치 증가로 인한 N_y 수치 증가인 경우
$W_{xy}<0$; N_x 수치 증가로 인한 N_y 수치 감소인 경우

그림 5. 퍼지인식도
Fig. 5. Fuzzy Cognitive Maps

판단모듈에서 여러 가변 요소 중 어떤 요소에 의존성을 부여함으로써 가장 최적의 탐지를 할 수 있는 것이 가장 큰 관건이다. 그뿐만 아니라 탐지한 IP address를 침입시도로 간주하고 블랙리스트 DB에 저장하여야 하는지도 결정하여야 한다. 퍼지인식도는 이러한 여러 가변 요소를 적용하여 최적의 판단을 내리게 한다[10, 11].

그림 6은 가변요소를 적용한 판단모듈의 퍼지인식도를 나타낸 것으로써, 판단모듈에 의존성을 갖는 가변요소로 IP address의 동일성 여부와 'half open state'의 시간간격 그리고 각 프로세서의 CPU가용율과 메모리가용율 및 판단모듈 후 재차 공격시 대응모듈의 처리로 인한 공격성 IP address에 대한 syn 패킷 조절을 둘 수 있다.

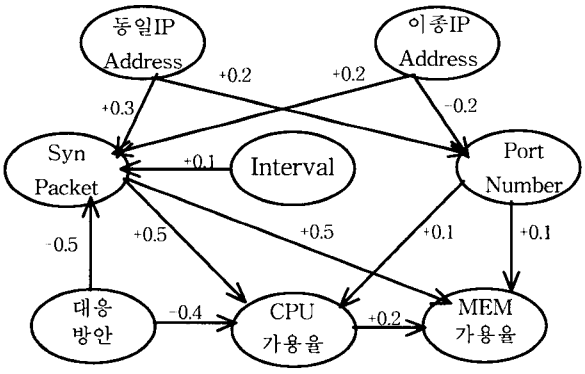


그림 6. 퍼지인식도가 적용된 판단모듈
Fig. 6. Decision Module Using FCM

가변요소를 노드(N_x)와 다음 노드(N_y)에 두고 두 노드의 링크인 가중치(W_{xy})를 적용하는 것이다. 예를 들면, Syn Packet과 CPU가용율에서는 Syn Packet의 용량이 증가할수록 CPU가용율이 증가하므로 이때 가중치는 0보다 크게 된다. 이때 임의의 노드에 가해지는 수치는 노드와 가중치를 연결한 네트워크를 통과할수록 그리고 반복횟수에 따라서 달라지게 된다. 이를 수식화 하면 식 (1)과 같다.

$$N_k(t_{n+1}) = \sum_{i=1}^{n} W_{ik}(t_n) N_i(t_n) \quad (1)$$

단, 가중치(W_{xy})의 증감부호는 다음 노드에 미치는 영향에 따라서 결정을 내렸으며 수치는 의미 있는 규칙기반에 의한 수치를 정하기 위해 연구를 하고 있으며 현재로는 반복적 실험에 의한 경험치를 사용하여 시험망에서 테스트를 하였다. 테스트를 한 결과, 공격횟수 0~70,000번으로 공격이 증가할수록 하드웨어가용율(CPU와 메모리)이 최종적으로 시스템부하로 적용되며 시스템부하율의 변화추이로 최대침입시도공격시 시스템 위험도를 확인할 수 있게 된다.

그림 7에서 침입시도시 하드웨어 가용율의 임계값 및 침입시도 판단 및 결정하는 데드라인으로 40% 가용율영역대를 설정하고 60% 가용율영역대를 시스템관리자에게 통보하는 임계값으로 설정한다. 이는 실시간 대응처리를 고려한 수치와 시험망이 아닌 네트워크에서 분산 서비스 거부공격(DDoS)을 위해 감안한 수치이며 반복적 테스트에 의한 평균값을 적용하였다[11].

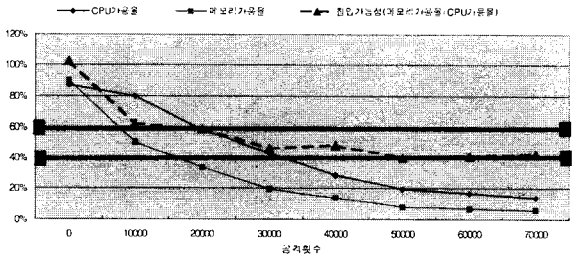


그림 7. 시험망에서의 공격횟수에 대한 하드웨어 가용율
Fig. 7. Attack Numbers vs. Hardware Capacity on Testbed Network

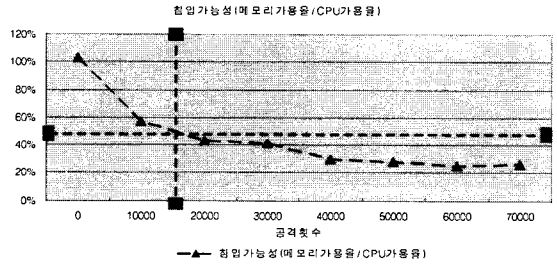


그림 8. 실시간 네트워크에서의 공격횟수에 대한 하드웨어 가용율
Fig. 8. Attack Number vs. Hardware Capacity on Real Time Network

그림 7에서 공격횟수가 50,000번 이상인 경우 시스템의 부하율이 데드라인을 넘게된다. 그러나 실제 네트워크에서는

그림 8에 나타나듯이 테스트결과보다 더 낮은 공격횟수에서 발생하였는데, 초당 16,000번 이상으로 interval을 불규칙적으로 발생하였을 경우 시스템부하율이 50%보다 낮은 수치를 보였다. 이런 결과는 실제 네트워크에서 발생할 수 있는 여러 가능 요소인 트래픽, 전파지연시간 그리고 hop count를 무한루프로 돌리는 패킷 등에 대한 고려사항을 감안하지 않은 결과로 본다[7].

실제 네트워크상의 테스트는 2002년 9월 3주 동안의 결과를 나타낸 것이며 100Mbps 카테고리 5의 이더넷환경에서의 인텔펜티엄4 2GHz, DDR 512M 시스템과 시스코 라우터 1750시리즈 그리고 RADCOM Ltd의 RC-100WL High-performance WAN/LAN 프로토콜 분석기에서 측정하였다. 표 1은 측정 일자 및 측정시각과 시간을 나타낸 것이다.

표 1. 실시간 네트워크상에서의 테스트 일정
Table 1. Test Time-Schedule on Real Time Network

일 자	측정 시각(h)				측정 시간
2002.09.1week	00	09	15	20	1 시간
2002.09.2week	00	09	15	20	1 시간
2002.09.3week	00	09	15	20	1 시간

3.3 대응모듈

대응모듈은 네트워크의 접근통제를 기본으로 하였으며 제안하는 모듈은 공격자 접근통제 알고리즘을 이용한 것이다[12]. 사용자의 접근통제 정보로는 데이터링크 계층에서의 Source MAC Address와 Destination MAC Address, 네트워크 계층에서는 TTL(Time to Live) 정보와 Source IP address, Destination IP address 그리고 전송 계층에서는 Tcp Source Port와 Tcp Destination Port가 필요하다.

3.3.1 IP Address 와 MAC Address의 비교

네트워크에 있는 시스템은 MAC Address를 가지며 외부에서 들어오는 모든 패킷은 게이트웨이의 MAC Address를 가지게 하여 접속을 시도하는 MAC Address가 게이트웨이의 MAC Address와 동일하면 공격으로 간주하는 것이다. 주소가 동일한 경우 공격으로 간주하여 액세스 거부를 하며 그렇지 않은 경우 액세스를 허용하는 것이다.

[Src_IP_Add ⊂ Group_IP_Add] &
[MAC_Src_Add == MAC_Router_Add] -->Attack

3.3.2 IP Address 불허 서비스

여기서는 미리 허용하는 IP 주소와 불허하는 IP 주소를 지정하고 허용된 IP 와 Port이면 허용하고 그렇지 않으면 불허하는 것이다.

[Src_IP_Add ⊂ Allow_IP_Add] -->허용
[Src_IP_Add ⊂ Deny_IP_Add] -->불허
[Dest_IP_Port ⊂ Allow_Port] -->허용
[Dest_IP_Port ⊂ Deny_Port] -->불허

4. 결론

본 논문에서는 Syn Flooding attack에 대해서 살펴보았으며 해결책으로 여러 대안 중에서 backlog_queue와 syncookies 수치를 조절한 1차 해결안을 채택하였다. 아울러 데이터링크계층의 패킷을 캡쳐 및 분석하여 침입시도탐지기능을 수행하는 네트워크 기반 탐지모델을 제안하고 시험망에서 테스트하였다. 여기서, 탐지성능을 좌우하는 요소들간의 상호 관계로부터 퍼지인식도를 이용한 침입시도 여부를 판단하였는데, 퍼지인식도에서 가장 중요한 가중치를 결정하는 수치에 대해서는 연구가 진행중이나 현 시점에선 반복 실험치에 근거를 두었다. 아울러, 침입시도 여부를 판단하는 하드웨어 가용용량 구역대(40%~60%)를 정확히 선정하기 위하여 실시간 처리 가능한 데드라인 시간과 초당 발생하는 Flow 임계값을 설정하여 침입여부를 결정하는 실험도 병행하여 진행 중이다.

향후 연구과제로 패킷캡처와 분석 및 판단모듈을 각각의 독립시스템에 두고 현재의 FCM를 개선하여 시험망과 실제 네트워크상에서 테스트를 하며 이와 병행하여 다른 접근방법론을 통한 판단결정모듈을 더욱 세분화한 탐지모델을 연구중이다. 그리고, 접근통제를 이용한 블랙리스트DB와 비교를 통한 대응모듈은 지능적으로 학습화된 개선된 대응모듈로 발전시킬 것이며 이를 기반으로 한 실시간 탐지 및 방지시스템으로 발전하는 것을 연구 목표로 삼는다.

참 고 문 헌

[1] Computer Emergency Response Team, "TCP Syn Flooding and IP Spoofing Attacks," CERT Advisory: CA, 96-21, 1996.

[2] Syncookies mailing list. ftp://koobera.math.uic.edu/pub/docs/syncookies-archive, 1996.

[3] SEC-INFO mailing list. http://www.certcc.or.kr/mail-archive/si-mail/0184.html, 2001.

[4] Y. W. Chen, "Study on the prevention of SYN flooding by using traffic policing," Network Operations and Management Symposium, 2000, IEEE/IFIP, pp. 593-604, 2000.

[5] C. K. Fung and M. C. Lee, "A denial-of-service resistant public-key authentication and key establishment protocol," Performance, Computing, and Communications Conference, 2002. 21st IEEE International , pp. 171-178, 2002.

[6] D. M. Gregg, W. J. Blackert, D. V. Heinbuch and D. Furnanage," Assessing and quantifying denial of service attacks," Military Communications Conference, 2001, Communications for Network-Centric Operations: Creating the Information Force. IEEE , Vol. 1, pp. 76-80, 2001.

[7] Ming Li, Weijia Jia, Wei Zhao, "Decision analysis of network-based intrusion detection systems for denial-of-service attacks," Info-tech and Info-net, 2001. Proceedings. ICII 2001 - Beijing, 2001 International Conferences on , Vol. 5, pp. 1-6,

2001.
[8] C. L. Schuba, I. V. Krsul, M. G. Khun, E. H. Spaford, A. Sundram, and D. Zamboni, "Analysis of a denial of service attack on tcp," 1997 IEEE Symposium on Security and Privacy, 1997.
[9] Aman Garg and A. L. Narasimha Reddy, "Policy Based End Server Resource Regulation," IEEE/ACM Transactions on Networking, Vol. 8, No. 2, pp. 146-157, 2000.
[10] S. Y. Lee and Y. S. Kim, "A RTSD Mechanism for Detection of DoS Attack on TCP Network," Proceedings of KFIS 2002 Spring Conference, pp. 252-255, 2002.
[11] K. B. Sim , J. W. Yang, D. W. Lee, S. Y. Lee, Y. S. Kim, et al., "Intrusion Detection System of Network Based on Biological Immune System," Journal of Fuzzy Logic And Intelligent Systems, Vol. 12, No. 5, pp. 411-416, 2002.
[12] E. J. Lee. " A Study on Intrusion Detection System through Network," Master Thesis, Inchon University, pp. 56-60, 2001.

저 자 소 개

이세열(Se-Yul Lee)
1996년 : 대전대학교 전자물리학과 이학사
1999년 : 동 대학원 정보통신공학과 공학석사
2000년 : (주)인소팩 부설기술연구소 연구원
2003년 : 동 대학원 컴퓨터공학과 박사수료

관심분야 : 침입탐지, 정보보호, 네트워크 보안, 퍼지 논리, 신경회로망 등
Phone : +82-42-280-2540
Fax : +82-42-284-0109
E-mail : ailab@dju.ac.kr

김용수(Yong-Soo Kim)
1981년 : 연세대학교 전기공학과 공학사
1983년 : KAIST 전기 및 전자공학과 공학석사
1986년 : 삼성전자 종합연구소 주임연구원
1993년 : Texas Tech Univ. 공학박사
1995년~현재 : 대전대학교 컴퓨터공학부 부교수

관심분야 : 신경회로망, 퍼지 논리, 패턴인식, 영상처리, 침입탐지 등
Phone : +82-42-280-2547
Fax : +82-42-284-0109
E-mail : kystj@dju.ac.kr

심귀보(Kwee-Bo Sim)
1984년 : 중앙대학교 전자공학과 공학사
1986년 : 동 대학원 전자공학과 공학석사
1990년 : The University of Tokyo 전자공학과 공학박사
2003년~현재 : 한국퍼지 및 지능시스템학회 부회장
2001년~2002년 : 대한전기학회 제어및시스템 부문회 편집위원 및 학술이사
2000년~현재 : 제어자동화시스템공학회 이사
1991년~현재 : 중앙대학교 전자전기공학부 교수

관심분야 : 인공생명, 진화연산, 지능로봇시스템, 뉴로-퍼지 및 소프트 컴퓨팅, 자율분산시스템, 로봇비전, 진화하드웨어, 인공면역계 등
Phone : +82-2-820-5319
Fax : +82-2-817-0553
E-mail : kbsim@cau.ac.kr