네트워크 패킷 분석을 기반으로 한 실시간 서비스 거부 공격 탐지 알고리즘

이 경 하[†] · 은 유 진[††] · 정 태 명[†††]

요 약

네트워크 기반에서 시도되는 최근 공격 유형들은 시스템과 네트워크의 정상적인 동작을 방해하는 간접적 형태의 공격 들이 점차 증가 추세를 이루고 있다. 본 논문에서는 네트워크 패킷을 기반으로 시도되는 여러 유형의 간접 공격들 중 네트워크 계층에서 이루어지는 서비스 거부 공격에 대한 분석과 공격 특징에 따른 유형들을 분류하고 이를 탐지할 수 있는 방법들을 제시하였다. 또한 단일 알고리즘으로부터 다양한 유형의 공격들을 탐지 할 수 기능과 추가적인 탐지 기능의 확장성 등을 제공할 수 있는 효율적인 통합 서비스 거부 공격 탐지 알고리즘을 설계하였다.

Real-Time Denial of Service Detection Algorithm Based on Analysis of Network Packets

Kyung-Ha Lee[†] · You-Jin Eun[††] · Tai-Myoung Chung[†††]

ABSTRACT

Recently, increasing attacks using network packets cause serious problems in networked environments; from disturbing normal network operations to damaging computing resources. Among them denial of services are considered as critical attacks that directly exploit network packets to degrade availability. In this paper, we classify the types of denial of services in the network layer and develop detection methods that can keep the network from the classified denial of service attacks. The methods are then merged into an integrated denial of service detection algorithm that is scalable to detect new denial of service attacks.

1. 서 론

인터넷은 현대 기술의 발전과 더불어 꾸준히 성장을 해왔으며, 다양한 인터넷 프로토콜과 이를 기반으로 하는 많은 종류의 인터넷 서비스들은 그 응용 범위가 확장되면서 기업이나 사회의 전분야에 걸쳐 많은 사용자들이 쉽게 인터넷을 활용할 수 있게 되었다.

그러나 이러한 인터넷의 활용성, 편리성을 발판으로 한 인터넷의 성장과정 이면에는 보안과 관련한 인터넷의 역기능 현상에 대한 위험은 계속해서 존재해 왔다. 따라서 많은 연구 개발자들이 시스템이나 개인정보의 보안을 위해 네트워크나 시스템에서의 보안 도구 개발과 다양한 보안 알고리즘 개발에 관심을 갖고 연구를 추진해 왔다.

고전적인 형태로서 보안을 위협하는 공격 유형은, 시스템의 취약점이나 프로그램의 버그를 이용한 침입,

† 준 회 원 : (주)데이타게이트 인터내셔널 보안기술 연구소 연구원
†† 비 회 원 : 한국정보통신기술협회 시스템보안연구위원회 연구위원
††† 종신회원 : 성균관대학교 전기전자 및 컴퓨터공학부 교수

논문접수 : 1998년 9월 30일, 심사완료 : 1999년 6월 19일

불법적으로 시스템 접속 후 시스템 내부 자원들에 대한 조작과 같은 직접적인 공격 형태 등이 대부분이었다. 그러나 점차 시스템과의 접속으로부터 발생되는 직접적인 공격 형태보다는 특정 프로토콜의 패킷을 이용한 간접적인 형태의 공격을 시도하여 정상적인 시스템 동작이나 네트워크 서비스를 방해하는 간접적인 유형의 공격들[15][18]이 증가하고 있다.

본 논문에서는 이러한 간접적인 공격 유형들 중 네트워크 상에서 패킷을 이용하여 시도되는 여러 유형의 서비스 거부 공격(Denial Of Service Attack)들을 각 유형별로 분류하고 이를 하나의 통합된 알고리즘으로부터 각각의 공격 유형들을 탐지할 수 있는 방법을 제시하고자 한다. 본 논문의 구성은 2절에서 서비스 거부 공격에 대한 정의와 침입 유형들을 정리하고, 이로부터 확인된 공격 유형의 탐지 방법들을 제시한다. 3절에서는 기존의 공격 유형 분석을 바탕으로 통합된 서비스 거부 공격 탐지 알고리즘 구현과 그 내부 모듈들에 대한 기능들을 설명하고, 4절에서는 제안된 서비스 거부 공격 탐지 알고리즘에 대한 분석과 효율성에 대하여 언급한다. 마지막으로 5절에서는 제안된 알고리즘에 대한 활용방안과 추후 계속적으로 본 연구와 관련되어 진행되어야 할 방향을 제시함으로써 끝을 매듭짓는다.

2. 서비스 거부 (Denial Of Service:DOS) 공격

서비스 거부 공격이란 '공격 대상 시스템/네트워크의 자원을 독점 혹은 파괴함으로 시스템이나 네트워크가 정당한 사용자들에게 올바른 서비스 제공을 하지 못하게 하거나, 정보 전송을 방해하는 행위'로 정의할 수 있다[3][16][18]. 서비스 거부 공격 방법은 크게 두 가지로 분류될 수 있는데 시스템 내부로 접속 후 시스템 내부 자원들에 대한 직접적인 공격을 시도하는 유형과 네트워크 패킷을 이용하여 네트워크 혹은 네트워크로 연결된 특정 시스템의 각종 서비스들의 정상적인 동작을 방해하는 간접적인 공격 유형이 있다[18]. 본 논문에서는 두 가지의 서비스 거부 공격 유형들 중 네트워크 패킷들을 기반으로 하는 서비스 거부 공격을 중심으로 기술한다.

2.1 서비스 거부 공격 유형

일반적으로 네트워크를 이용한 공격들은 내부 네트워크의 시스템들을 대상으로 시도된다. 공격 유형으로는 일련의 패킷을 이용한 공격, 침입에 취약한 네트워크 서비스 혹은 포트를 이용한 공격, 그리고 특정 경로를 이용한 우회 침투 등과 같은 공격들이 있다[2][18].

그러나, 이러한 공격 유형들 중 서비스 거부 공격은 네트워크를 이용한 공격기술을 보다 고급화한 공격유형으로 호스트 뿐 아니라 게이트웨이나 네트워크 환경으로 공격 대상의 영역을 확장한 것이다. 이와같이 네트워크 상에서 시도되는 서비스 거부 공격 방법들을 특징별로 살펴보면, 아래와 같이 4가지의 형태로 분류할 수 있다.

2.1.1 Insertion(삽입)

삽입에 의한 서비스 거부 공격은 두 가지 유형으로 나눌 수 있다. 먼저, 첫번째는 비정상 값 삽입 공격 유형(Abnormal Value Insertion Attack Type)으로 네트워크 패킷 헤더의 체크섬(checksum), 옵션(option) 등의 필드에 비정상적인 값을 삽입하거나, 전송하는 패킷에 적절치 않는 네트워크 옵션을 설정하여 패킷을 전송하는 공격 유형이다[11][17]. 두 번째 유형은 비 정상적인 패킷 삽입 공격(Abnormal Packet Insertion Attack Type)으로 Packet Sniffing을 통하여 두 시스템 사이에서 전송되는 일련의 패킷들 사이에 비정상적인 패킷을 삽입하는 공격 유형이다[11][17].

비정상 값 삽입 공격은 전달되는 패킷이 게이트웨이나 전송된 시스템에서 연속적인 중지를(packet drop) 발생시켜 시스템의 성능저하를 가져올 수 있으며, 비정상적인 패킷 삽입 공격 유형은 정확한 정보 전송에 오류를 발생시켜 시스템의 오 동작을 유발할 수 있다.

2.2.2 Oversize(비대)

Oversize 공격 유형은 송/수신되는 패킷의 전체 크기를 조작하여 수신측이 감당할 수 없는 크기의 패킷을 전송함으로 시스템의 정지와 같은 문제를 발생시키는 공격 유형이다. [11][17]

2.2.3 Traffic Flooding

Traffic Flooding을 이용한 서비스 거부 공격 유형은 호스트 혹은 네트워크 간에 데이터 교환을 위해 생성되는 정상적인 패킷 이외에도, 단시간에 다량의 비정상적인 패킷들을 생성하여 네트워크 패킷의 교통량을

급증시키는 공격 유형이다[4][8][10]. 이러한 서비스 거부 공격은 네트워크 자원을 고갈시킬 뿐 아니라, 최악의 경우에 있어서는 목표 대상의 시스템 동작을 마비시키는 역기능 현상을 가져온다.

2.2.4 Disconnection

Disconnection공격은 패킷들을 교환하는 일련의 과정에서 비정상적인 패킷을 생성 혹은 패킷 전송에 필요한 중간 과정을 방해 함으로 시스템이 정상적인 네트워크 서비스를 사용할 수 없도록 하는 공격 유형이다[1][4][12].

특히 TCP 프로토콜 취약성을 이용하여 시도되는 공격 유형으로 Three Handshake 패킷 전송 방법[19]에서 패킷 전송의 중간 과정을 생략하거나 비 정상적인 패킷을 삽입하여 현재의 연결을 강제로 해제한다.

2.2 서비스 거부 공격 탐지 방법

본 절에서는 앞에서 분류된 네트워크 패킷을 이용한 서비스 거부 공격 유형들의 탐지하기 위하여 다음과 같은 네 가지 방법을 제시하고자 한다.

2.2.1 Value Comparison

서비스 거부 공격을 탐지하기 위하여 관리자/시스템으로부터 설정된 기준 값이나 데이터들의 유효치를 벗어나는 경우를 탐지하는 방법이다.

(1) Address Comparison : 패킷 전송을 위하여 패킷 헤더에 입력된 전송지와 목적지의 주소들과 데이터 베이스에 입력된 자료와의 비교를 통하여 공격 여부를 확인하는 방법이다[18].

이 방법은 내부 네트워크 사용자들로부터 Spoofing[1] [5][14]을 이용한 서비스 거부 공격을 탐지하는 데 유용하며 외부 네트워크에 대하여서도 위험 지역의 주소지로부터의 접속 탐지, 내부 네트워크의 특정 호스트를 보호할 목적으로 인증되지 않은 로컬 및 외부 호스트로부터의 접근을 탐지하는 일반 네트워크 상의 침입탐지 기능을 제공한다.

(2) Abnormal Value Comparison : 패킷 헤더와 패킷 자체 크기의 조작을 통한 서비스 거부 공격을 탐지하는 방법이다[17]. 패킷 헤더의 특정 필드에 삽입된 값을 점검하여 기준 허용치를 벗어난 경우와 패킷 자체의 크기가 조작되어 목적지로 패킷을 전송되는 공격을 탐지한다.

2.2.2 Field Checking

네트워크 상에서 사용되는 일부 프로토콜중에서 패킷 헤더의 특정 옵션 필드가 설정 됨으로써 서비스 거부 공격으로 이용되는 것을 탐지하는 방법이다[11][17].

2.2.3 Time & Counting

Time & Counting은 정상적인 네트워크 서비스로부터 발생되는 패킷의 주기, 트래픽과 공격의 의도로서 발생되는 서비스 거부 공격을 구별할 수 있어 공격 탐지에 정확성을 제공할 수 있다.

(1) Packet Counting : 패킷 트래픽을 이용한 공격을 탐지하기 위한 방법으로 일부 네트워크 서비스에 사용되는 패킷들을 특정 호스트나 네트워크 전체로 전송되는 패킷의 수량을 점검하여 침입을 탐지하는 방법이다.

(2) Packet Timing : Packet Counting 방법과 함께 사용하여 트래픽을 이용한 서비스 거부 공격을 탐지한다. 패킷의 전송주기를 정상적인 패킷 전송과 서비스 거부 공격을 구별할 수 있는 조건으로 사용하여서 서비스 거부 공격 탐지의 정확성을 높인다.

2.2.4 Connection Inspection

정상적인 세션설정 및 데이터 교환을 방해하는 서비스 거부 공격을 탐지하는 방법이다.

일부 프로토콜에서 네트워크 서비스를 사용하려면 세션 설정과 데이터 교환 시 일련의 접속 단계가 요구된다. 이 과정 중에서 한 부분이 생략, 중복되거나 다량의 비 정상적인 패킷이 생성되면 시스템에 문제가 발생하게 된다. 이러한 유형의 침입을 탐지하기 위하여 연결 설정/해제, 혹은 데이터 전송 과정에서 정상적인 연결 및 데이터 전송 유무를 확인한다. 이와 관련하여 시도되는 공격 유형으로는 TCP Connection에서 Sync Flooding[9][13], TCP접속 끊기[12] 등이 있다.

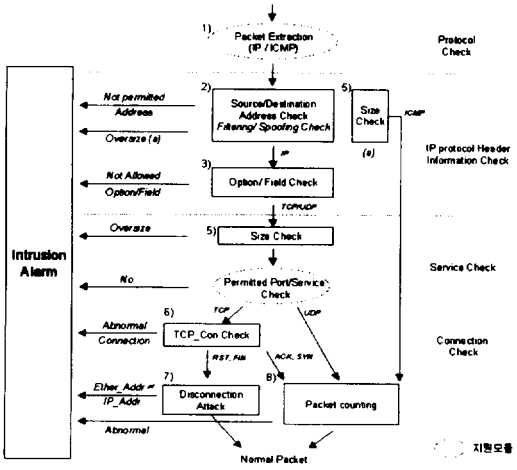
3. 서비스 거부 공격 탐지 알고리즘(Denial Of Service Detection(DOS) Algorithm)

본 장에서는 2장에서 언급한 여러 유형의 탐지 방법

1) 내부 네트워크에서 IP address는 Spoofing 과 같은 공격으로부터 목표 호스트로의 조작된 패킷 전송을 판별하기 위해 Ethernet address(MAC address)와의 비교과정이 추가될 수 있다.

들을 보다 세부 모듈로 설계하여 서비스 거부 공격을 탐지할 수 있는 통합 알고리즘을 제시하고자 한다. 특히 효율적인 알고리즘의 설계를 위해 순수 서비스 거부 공격 탐지 모듈에 네트워크 기반의 일반 침입 탐지의 지원 모듈을 추가함으로 서비스 거부 탐지 알고리즘의 성능 및 효율성 높일 수 있도록 하였으며, 일부 모듈에서는 서비스 거부 공격 탐지 모듈의 기능과 지원 모듈의 기능 모두를 포함하도록 설계하였다.

(그림 1)은 2.2에서 언급한 각각의 DOS 탐지 방법들을 하나의 통합된 DOS 탐지 알고리즘으로 나타낸 것으로, 이것은 알고리즘이 적용하게 될 네트워크에서 서비스 거부 공격과 관련된 패킷을 추출하는 과정을 시작으로, 마지막 단계에서 비 정상적인 패킷이 아님을 판정하기까지의 과정을 기능별 혹은 계층별로 나타내고 있다.



(그림 1) 서비스 거부 공격 탐지 알고리즘

3.1 모듈 분석 : DOS 탐지 모듈과 지원 모듈

DOS Detection Module은 직접적으로 DOS를 탐지하는 모듈로서 DOS 공격 유형과 관련된 프로토콜에 따라 기능별로 분류되어 동작한다.

지원 모듈은 (그림 1)에서 타원으로 표시한 부분으로 패킷 필터링, 패킷 헤더의 조작이나 취약한 서비스를 이용한 단순한 침입 유형의 탐지, 그리고 패킷 추출(Packet Extraction)과 같은 기능을 제공한다. 이러한 기능들은 최소의 침입 관련 자료로부터의 공격 탐지와 다양한 보안 규칙을 적용할 수 있게 함으로 알고리즘의 효율을 높일 수 있다.

3.2. DOS 탐지 세부 모듈의 기능

(그림 1)에서 통합 DOS 탐지 알고리즘을 구성하고 있는 각 세부 모듈들에 대한 기능들은 다음과 같다.

3.2.1 Packet Extraction(IP/ICMP)

Packet Extraction모듈은 통합 DOS 탐지 시스템의 효율성 향상과 관련된 지원 모듈이다. 이 모듈의 역할은 탐지하고자 하는 DOS 공격과 관련된 프로토콜 패킷만 추출하여 공격 탐지 대상 패킷의 규모를 축소한다. 즉, 서비스 거부 공격과는 관련성이 적은 프로토콜을 탐지 대상에서 제외하고, IP나 ICMP같이 공격의 가능성이 높은 패킷만을 알고리즘에 적용시킴으로 DOS 탐지 알고리즘의 효율성을 높이는 기능을 한다.

3.2.2 Source/Destination Address Check

Source/Destination Address Check 모듈은 서비스 거부 공격 탐지 기능과 일반적인 네트워크 보안 기능을 함께 제공한다. 이 모듈은 <표 1>에서 나타낸 것과 같이 네 가지 탐지 기능을 제공하는데, 앞의 두 개의 모듈은 지원 모듈로서 뒤의 두 개의 모듈은 순수한 서비스 거부 공격 탐지 모듈로서 제공된다.

<표 1> Source/Destination Address Check 모듈 기능

Source/Destination Address Check
- Supporting Module
• Address Filtering
• Simple Authentication Apply with DNS
- DOS Detection Module
• Adding Intrusion Detection for Specified Address
• Spoofing Detection in Local Network

본 모듈의 세부 기능들은 다음과 같다. 첫째는 관리자가 사전에 취득한 보안 정보로부터 공격의도가 높은 네트워크 혹은 호스트로부터의 접근과 보안 등급이 높게 설정된 특정 호스트로의 접근을 탐지하는 주소 필터링(Address Filtering) 기능, 둘째는 네트워크 주소가 DNS에 등록되어 있지 않은 주소를 탐지함으로 단순한 인증절차[2]를 제공한다. 셋째는 특정 호스트나 네트워크 주소로부터 전송되는 패킷만을 대상으로 추가적인 서비스 거부 공격 탐지 모듈을 실행하는 기능을 제공

2) Simple Authentication Apply with DNS 기능은 Domain Name Server에 등록되어 있는 주소들만을 인증된 호스트임을 전제로 한다.

하며, 넷째로는 공격 탐지 대상을 내부 네트워크에 있는 호스트들로 한정하고 Ethernet Address와 IP Address를 확인하여 조작된 주소를 사용한 접속을 탐지한다.

이러한 기능들은 일반적으로 공격자가 DOS 공격을 시도할 때 패킷 헤더에 포함되는 주소지에 대한 조작이 함께 이루어지는 것[5][14]을 고려한 것으로, DOS 공격 탐지에 보다 정확성을 제공한다.

3.2.3 Option/Field Check

네트워크 패킷들을 대상으로 패킷의 헤더 정보 중 서비스 거부 공격을 목적으로 패킷의 특정 필드 옵션을 설정한다든지, 헤더 필드에 삽입되는 지정된 값을 기준치 이상 혹은 이하의 값으로 조작하여 목적지 호스트나 네트워크로 전송하는 패킷을 탐지 한다. 'Insertion공격' 유형은 이 모듈부터 탐지된다.

3.2.4 Permitted Port/Service Check

지원 모듈 중 하나인 Permitted Port/Service Check는 특정 서비스나 포트를 대상으로 트래픽을 이용한 서비스 거부 공격들의 징후에 대한 포착과 TCP/UDP 프로토콜을 기반으로 하는 네트워크 패킷들 중 이미 발표된 여러 보안 문서들로부터 침입에 취약한 것으로 평가되어 네트워크 관리자로부터 사용이 허가되지 않는 네트워크 서비스를 사용하려는 시도를 탐지한다.

3.2.5 Size Check

Oversize를 이용한 서비스 거부 공격을 탐지하는 모듈로서, 수신측이 수용할 수 없는 조작된 크기의 패킷을 전송하는 공격을 탐지한다..

3.2.6 TCP_Con Check

TCP 프로토콜의 데이터 전송에 따른 특징을 이용한 서비스 거부 공격 유형들을 탐지하는 모듈로서, 모든 TCP 세션에 대한 감시로부터 정상적인 TCP 연결 설정의 유무를 확인한다. 특정 서버로의 과잉 TCP Connection 생성, Half open된 TCP 연결 설정을 점검한다.

3.2.7 Disconnection Attack

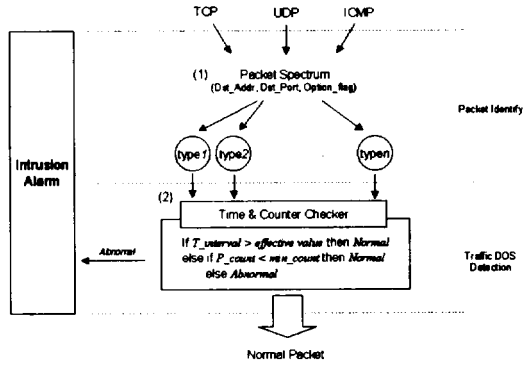
TCP 프로토콜의 취약성[1][13]을 이용한 DOS 공격 탐지를 하는 모듈이며, 현재 설정되어 있는 세션(session)을 강제로 해제 시키는 공격 유형들을 탐지한다.

공격자는 이미 네트워크 상에 연결되어 있는 TCP 세션을 임의의 로컬 호스트에서 패킷 Sniffing을 이용하여 필요한 정보를 취득한 후, 패킷 전송지의 네트워크 주소로 위장된 한 개 이상의 "RST", "FIN" 플래그가 설정된 TCP 패킷들을 목적지에 보내어 현재 사용중인 세션을 강제로 해제 시킨다. 이러한 유형의 공격은 Ethernet 주소의 확인 과정으로부터 정상적인 주소지로부터의 보내진 TCP 패킷 여부를 확인함으로 탐지할 수 있다. 그러나 이 방법은 내부 네트워크의 호스트들 사이에서 시도되는 Disconnection 공격 만을 탐지할 수 있다는 한계가 있다.

3.2.8 Packet Counting

앞서 언급한 모듈들에서는 서비스 거부 공격 여부를 확인하기 위하여서 작게는 한 개에서부터 수십 개의 특정 패킷들이 사용되었으나, Packet Counting 모듈에서는 최소 수십 개에서 수천 개 이상의 패킷들이 서비스 거부 공격 여부를 탐지하는데 요구된다.

(그림 2)는 (그림 1)에서의 Packet Counting 모듈의 상세도로서, TCP 패킷은 물론 UDP와 ICMP 패킷 모두를 공격 탐지 대상으로 한다. 보다 세부적인 모듈들의 기능은 다음과 같다.



(그림 2) Packet Counting 모듈 상세도

(1) Packet Spectrum

Packet Spectrum 모듈은 패킷의 트래픽을 이용한 공격 유형을 각 프로토콜의 세션과 사용 서비스(혹은 포트)를 기준으로 분류한다. 이는 ACK Storm, UDP Echo(fraggle), ICMP echo(smurf), Finger, Chargen과

같은 특정 서비스 사용하여 일부 호스트나 네트워크를 대상으로 다량의 동일한 패킷들을 전송하는 공격을 탐지하기 위한 사전 작업을 수행한다.

이때 Source Address나 Source port는 Type 설정 기준에 포함하지 않는다. 이는 프로토콜, Destination Address (Destination port), 그리고 동일한 종류의 패킷 여부를 확인하기 위한 프로토콜의 일부 패킷 필드만을 사용하여 하나의 세션은 물론, 여러 개의 세션으로부터 특정 호스트나 네트워크 주소지로 집중되는 트래픽 공격을 탐지하기 위함이다.

<표 2>는 프로토콜별 Type 설정의 기준이 되는 분류 요소들이다

〈표 2〉 Packet Spectrum에 의한 프로토콜별 Type 분류

프로토콜	분류 요소들
TCP	Destination Address, Destination Port Option_Flag : ACK, ACK_Number / SYN
UDP	Destination address, Destination port
ICMP	Destination address, Option_Flag : Response, Request)

(2) Time & Counter Checker

Packet Spectrum으로부터 나뉘어진 각각의 Type들은 각각의 Type 별로 트래픽을 이용한 DOS 공격을 탐지한다. (그림 2)에서 Time & Counter Checker 모듈의 공격 탐지 규칙(Rule)은 <표 3>과 같이 정의된 변수들을 사용하여 적용된다.

〈표 3〉 Time & Counter Checker 변수 정의

변 수	특 징
T_interval	패킷들간(두개의 패킷들간)의 전송되는 시간 간격
Effective T_value	서비스 거부 공격의 의도로 간주 할 수 있는 T_value의 최대치를 설정, 서비스 거부 공격에 사용되는 패킷은 1초에 최소 1개에서부터 최대 천 개 이상의 동일한 패킷이 생성이 된다
P_couter	같은 유형(Type) 패킷으로 네트워크 상에서 전송되는 패킷 수
Min_count	서비스 거부 공격의 의도로 생성된 패킷이라 간주 할 수 있는 같은 유형의 최소 패킷 수

<표 4>에서는 지금까지 3장에서 설명한 (그림 1)의 통합 DOS 탐지 알고리즘의 세부 모듈에 대한 기능들을 2장에서 분류한 서비스 거부 공격 유형들과 각 유형별로 시도되는 공격 방법, 그리고 이를 탐지하는 본 알고리즘의 해당 모듈들의 관계를 정리하여 보았다.

〈표 4〉 네트워크 패킷을 이용한 서비스 거부 공격 유형 및 방법과 관련 자료

서비스 거부 공격 유형들	서비스 거부 공격 방법 및 관련 자료
Insertion (삽입)	IP spoofing attacks and hijacked terminal connections(CA : CERT/CC Advisories CA-95.01[3]) Teardrop_Land(CA-97.28.) Insertion Attacks by IP and TCP packet(Secure Network, Inc.[ ])
	관련 모듈 : Source/Destination Check, Option/Field Check, Normal TCP_Con Check
Oversize (비대)	Ping(CA-96.26) Oversize(KH98-041)
	관련 모듈 : Size Check
Traffic Flooding	UDP_service_denial(CA-96.01, Cisco : white paper, Caldera Security AdvisorySA-1997.33[4]) Tcp_syn_flooding(CA-96.21, Coast TR 97-06,) TCP Ack storms(Merit Network, Inc.) Smurf(CA-98.01)
	관련 모듈 : Permitted Port/Service Check, Packet Counting
Abnormal Connection Operation	IP spoofing attacks and hijacked terminal connections (CA-95.01) Tcp_syn_flooding(CA-96.21, Coast TR 97-06) Session Hijacking(KH : Korea Hacking test documentsKH98-022[5]) Disconnection attack(KH98-022,KH98-023)
	관련 모듈 : Source/Destination Check, Normal TCP_Con Check, Disconnection Attack

4. Prototype 구현

(그림 3)의 환경에서 본 알고리즘을 적용한 DOS 탐지 프로토타입은 10Mbps 이하의 로컬 네트워크에서는 패킷의 유실(loss) 없이 모든 탐지 모듈들이 동작 하였다. 그러나 점차 고속화 대용량화 되어가는 현 네트워크의 성장 추세를 고려할 때 100Mbps의 환경에서는 병목현상이 발생이 예상된다

5. 분 석

오늘날 서비스 거부 공격에 대한 관심은 다양한 공격 유형분석과 이를 탐지하기 위한 기술 중심의 연구

3) CA : CERT/CC Advisories
4) Caldera Security Advisory
5) KH : Korea Hacking test documents

로 이어졌고, 그 결과 이를 연구하는 여러 기관들로부터 많은 결과들이 나왔다. 구체적인 연구 결과로서 COAST 연구소와 Merit Network사에서 발표한 TCP의 취약성을 이용한 서비스 공격 분석[3][13], L. Todd Heberlein과 Matt Bishop의 특정 프로토콜에서의 Spoofing을 이용한 침입 유형과 탐지 방법[14], 그리고 ISS[11]와 Secure Network사[17]의 네트워크 기반에서 시도되는 침입 유형 분류와 특징 및 탐지 방법 등의 연구 성과와 이를 바탕으로 보안 권고문[2][5][6] 이나 보안 기술 문서들[4][7][12] 그리고 보안 도구들이 개발되었다.

그러나, 이러한 연구 결과들은 일부 특정 유형의 서비스 거부 공격에 대한 분석과 탐지 방법에 대한 연구 결과만을 제시할 뿐, 여러 유형의 서비스 거부 공격들을 모두 탐지할 수 있는 방법이나 통합 알고리즘에 대하여서는 구체적인 자료를 제시하지 못하고 있다. 따라서 본 논문에서는 앞에서 언급한 서비스 거부 공격 탐지의 8개 모듈로부터 네트워크에서 시도되는 서비스 거부 공격들을 탐지할 수 있는 통합적인 서비스 거부 공격 탐지 알고리즘에서 수용할 수 있도록 하였다.

5.1 효율성

시스템의 효율성을 위해 각 모듈들은 공격 탐지 시 패킷 필터링과 Reformat과정을 통하여 공격 탐지에 필요한 최소의 정보만을 사용한다.

5.2 단순성

침입 탐지를 위한 패킷 분석에 있어 네트워크 계층과 프로토콜에 따라 구별되는 공격 탐지의 특성을 반영하여 동일한 계층에서 여러 개의 유사한 특성을 갖는 침입 유형을 하나의 모듈에서 처리할 수 있도록 모듈 설계를 단순화하였다.

5.3 확장성

네트워크 계층별로 탐지 모듈들의 특징을 분류하여 설계하였다. 이러한 알고리즘은 나중에 추가될 모듈들에 대하여 손쉬운 확장성을 제공한다. 각 계층에서 추가될 모듈들과 현재는 TCP/IP의 프로토콜 계층 중 네트워크 계층(Network Layer)을 중심으로 서비스 거부 공격 탐지와 일부 네트워크 기반의 침입 탐지 기능을 제공하지만, 앞으로 응용계층에서의 이루어지는 서비스 거부 공격 탐지 모듈들은 현재의 알고리즘에 큰 수정 없이도 쉽게 추가 할 수 있다.

5.4 정확성

트래픽을 이용한 공격 탐지 기능을 강화한 설계로 특정 서비스를 이용한 트래픽 공격에 대하여 전송 패킷의 양과 전송 주기와 같은 탐지 요소를 설정하여 공격 탐지의 정확성을 높였다.

5.5 신뢰성

내부 호스트로부터의 공격들, Sniffing과 Spoofing을 이용한 공격에 대하여 실제 주소지로부터의 데이터 전송 여부를 확인함으로 통신에 있어 내부 네트워크에 대한 신뢰도를 높였다.

6. 결 론

본 논문에서 제안하는 서비스 거부 공격 탐지 알고리즘은 데이터 링크 계층으로부터 네트워크 계층의 정보들을 기반으로 각 탐지 기능별, 계층별로 모듈화 작업을 통하여 추후 확장될 기능들을 쉽게 반영할 수 있도록 설계하였다. 또한, 로컬 네트워크를 중심으로 기존의 특정 서비스 거부 공격 유형만을 대상으로 설계된 탐지 알고리즘들과는 달리 전반적인 서비스 거부 공격에 대한 유형들을 탐지 할 수 있도록 설계하였다.

그러나, 본 알고리즘은 네트워크에서 네트워크 계층을 중심으로 이루어지는 서비스 거부 공격에 대한 탐지 기능을 중심으로 설계된 것으로, 다각적인 공격이 이루어지는 응용 계층에 대한 침입 탐지와 외부 네트워크로부터의 일부 서비스 거부 공격에 대한 정확한 탐지와 추적이 어렵다는 단점이 있다. 따라서, 추후 연구 진행에 있어서는 외부 혹은 보안성 있는 통신을 필요로 하는 네트워크간의 상호 협조적인 보안 체계, 지원 시스템에 대한 연구, 기존의 네트워크 기반의 침입 탐지 시스템과의 통합, 공격에 대한 방어 기능, 그리고 응용 계층에서의 서비스 거부 공격에 대한 추가 및 탐지 알고리즘 확장과 관련된 연구가 요구된다. 그리고 침입 차단 시스템 및 기타 통합적인 보안 시스템으로의 확장성 등을 추가하여, 앞으로 이러한 연구 결과로부터 내부뿐만 아니라 전체 네트워크 보안 관리 체계에 있어 관리자에게 보다 강력한 네트워크 보안성을 제공할 수 있을 것이다.

참 고 문 헌

[1] Bellovin S.M., "Security Problems in the TCP/IP Protocol Suite," Computer Communication Review, Vol.19, No.2, pp.32-48, April 1989.

[2] Caldera Inc, "Vulnerabilities in inetd," Utah, 18 Dec. 1997, SA-1997.33.

[3] Christoph L. Schuba, Ivan Krsul, Markus Kuhn, E. H. Spafford, Aurobindo Sundaram, and Diego Zamboni, "Analysis of a Denial of Service Attack on TCP," IEEE Symposium on Security and Privacy; Oakland, CA; Coast TR 97-06; May, 1997.

[4] Cisco Systems Inc., "Defining Strategies to Protect Against TCP SYN Denial of Service Attacks," September, 1996.

[5] Computer Emergency Response Team(CERT), Carnegie Mellon University, Pittsburgh, PA., "IP Spoofing Attacks and Hijacked Terminal Connections," Jan. 1995. CA-95:01.

[6] Computer Emergency Response Team(CERT), Carnegie Mellon University, Pittsburgh, PA. "smurf," January 5, 1998, CA-98:01.

[7] Computer Emergency Response Team(CERT), Carnegie Mellon University, Pittsburgh, PA. "Teardrop_Land," December 16, 1997, CA-97:28.

[8] Computer Emergency Response Team(CERT), Carnegie Mellon University, Pittsburgh, PA. "ping," December 18, 1996, CA-96:26.

[9] Computer Emergency Response Team(CERT), Carnegie Mellon University, Pittsburgh, PA. "tcp_syn_flooding," September 19, 1996, CA-96:21.

[10] Computer Emergency Response Team(CERT), Carnegie Mellon University, Pittsburgh, PA. "UDP_service_denial," February 08, 1996, CA-96:01.

[11] Internet Security Systems(ISS), "RealSecure User's Guide and Reference Manual," 1996.

[12] Korea Information Security Agency(KISA), "Hacking Response Technique Handbook(KISA II-HE-981)," April, 1998.

[13] L.Joncheray, "A Simple Attack Against TCP," In 5th USENIX UNIX Security Symposium, June 1995.

[14] L. Tod Heberlein, Matt Bishop, "Attack Class : Address Spoofing," Proceedings of the 19th National Information System Security Conference pp.371-377.

[15] S. Cheung, K.N. Levitt, "Protecting Routing Infrastructures from Denial of Service Using Cooperative Intrusion Detection" Proc. New Security Paradigms Workshop 1997, Cumbria, UK, September 23-26, 1997.

[16] S. Garfinkel, G. Spafford, "Practical UNIX & Internet Security," O'Reilly & Associates, Inc, 1996.

[17] T. H. Ptacek, "Insertion, Evasion, and Denial of Service : Eluding Network Intrusion Detection," Secure Networks, Inc. Jan, 1998.

[18] V. Ahuja, "Network and Internet Security," Academic Press, Inc, 1996.

[19] W. R. Stevens, "TCP/IP Illustrated, Vol.1.," Addison-Wesley, Reading, MA, 1994.

이 경 하

e-mail : scott@datagate.co.kr

1997년 배재대학교 전자계산학과 (학사)

1999년 성균관대학교 전기전자 및 컴퓨터공학(석사)

1999년 1월~현재 ㈜데이타게이트 인터내셔널 보안기술 연구소 연구원

관심분야 : 네트워크/시스템 보안, 침입 탐지, 보안 관리

은 유 진

e-mail : silver@kisa.or.kr

1995년 아주대학 컴퓨터공학(학사)

1997년 아주대학교 컴퓨터공학(석사)

1996년 12월~현재 한국정보보호센터 기술개발부 연구원

1997년 10월~현재 한국정보통신기술협회 시스템보안 연구위원회 연구위원

관심분야 : 컴퓨터/네트워크 정보보호, 침입탐지시스템, 전자서명 인증기술

정 태 명

e-mail : tmchung@rtlab.skku.ac.kr

1981년 연세대학교 전기공학과(학사)

1984년 University of Ilinois Chicago, 전자계산학과(학사)

1987년 University of Illinois Chicago, 컴퓨터공학과(석사)

1995년 Purdue University, 컴퓨터공학(박사)

1985년~1987년 Bolt Bernek and Newman Labs., Staff Scientist

1995년~현재 성균관 대학교 교수

관심분야 : 실시간 시스템, 네트워크 관리, 보안 관리