향상된 침입 탐지 시스템을 위한 DoS 공격 유형의 분류 체계

김 광 득† · 박 승 균†† · 이 태 훈†† · 이 상 호†††

요 약

보안 공격에 대한 완벽한 방어 능력을 갖춘 시스템(IDS)은 없다. 왜냐하면 시스템의 모든 특성과 모든 공격 패턴을 수용한다는 것은 IDS 그 자체의 부하가 시스템에 많은 영향을 줄 수 있기 때문이며, 지능적으로 공격 패턴을 달리하는 많은 공격유형을 모두 인식할 수 없기 때문이다. 본 논문에서는 보다 효율적이고 실시간 탐지가 가능한 IDS 시스템을 위해 서비스 거부공격에 대한 새로운 분류 체계를 제안한다. 이는 목적 지향적 시스템이 시스템의 운영상태를 범용시스템에 비해 명확히 할 수 있다는 생각에서 출발되었으며 각 운영상태의 변화는 새로운 사건에 의해 기인되며, 이 사건이 어떠한 범주에 속하는지를 확인하여 분류 속성에 따른 침입탐지 시스템을 설계에 활용할 수 있다.

The Taxonomy Criteria of DoS Attack Pattern for Enhanced Intrusion Detection System

Kwang-Deuk Kim† · Seung-Kyun Park†† · Tae-Hoon Lee†† · Sang-Ho Lee†††

ABSTRACT

System(IDS) hasn't protection capability for various security attacks perfectly. Because, It is probably affected by IDS's workload caused by treating all kind of the characteristics and attack patterns of system and can't probe all of the attack types being intelligently different with attack patterns. In this paper, we propose a new taxonomy criteria about DoS(denial of service attacks) to make more efficient and new real time probing system. It's started with an idea that most of the goal oriented systems make the state of system operation more unambiguous than general purpose system. A new event caused the state of the system operation to change and classifying a category of the new events may contribute to design the IDS.

1. 서 론

현재의 많은 침입탐지 시스템(IDS : Intrusion Detection System)들은 많은 공격을 탐지하기 위해 사용자의 행위 변화 탐지, 잘 알려진 공격 패턴 탐지, 시스템의 결함점검 등을 통한 보편적이고 일반론적인 침입 탐지 시스템을 구현하고자 많은 연구를 하고 있다[1, 4, 7, 8]. 이러한 침입 탐지 시스템은 많은 양의 공격 정보 데이터 베이스를 필요로 하며, 공격에 대한 실시간 탐지에 많은 어려움이 있다. 또한 새로운 공격에 대한 탐지와 이를 데이터 베이스에 추가, 유지하는데도 많은 노력과 비용이 든다. 또한 1986년도 이후 서비스 거부(Denial of Service : DoS)공격의 지속적인 증가로 사이버 상거래의 역기능에 주요한 변수로 작용할 것으로 예상된다. 결국 침입 탐지 시스템의 위와 같은 문

† 준 회 원 : 한국에너지기술연구소 선임기술원
†† 준 회 원 : 충북대학교 대학원 컴퓨터과학과
††† 종신회원 : 충북대학교 컴퓨터과학과 교수
논문접수 : 1999년 8월 12일, 심사완료 : 1999년 10월 22일

제점을 해결하기 위해서는 공격 특성에 적합한 새로운 감시체계와 실시간 적이고, 새로운 공격 탐지도 가능한 침입 탐지 시스템이 필요하다(IDPS : IDS for DoS attack using Performance Signature)[10]. 또한, 이 IDPS를 구현하기 위해서는 DoS 공격에 대한 보다 실질적이고 정확하며, 시스템 성능을 대표할 수 있는 자원들을 기반으로 한 새로운 분류 체계가 필요하다.

따라서, 본 논문에서는 IDPS 구현의 첫걸음으로서, 시스템 자원을 기반으로 새로운 DoS 공격 유형 분류 체계를 제안한다.

이 논문은 제2장에서 DoS 공격의 유형과 일반적인 분류 체계를 살펴보고 제3장에서는 침입 탐지 모델의 특성에 맞는 새로운 분류법을 제시하며, 제4장에서는 분류체계가 지녀야할 특성을 만족하는지를 검증하고, 제안된 분류법이 적용될 수 있는 침입탐지 모듈의 구조를 보인다. 마지막으로 제5장에서는 결론을 맺는다.

2. DoS 공격

컴퓨터 시스템에서 모든 사용자가 바라는 가장 기본이 되는 보안 사항은 바로 가용성이다. 만일, 하드웨어와 소프트웨어 그리고 데이터가 가용성을 유지하지 못한다면, 아무리 외부의 침입으로부터 안전하다고 하더라도 그 생산성은 떨어질 것이다. 따라서 DoS 공격의 정의는 "의도적 또는 비의도적으로 시스템의 가용성을 떨어뜨리려는 공격"으로 정의할 수 있다. 다른 사용자의 의도적인 잘못된 행위의 결과로써, 컴퓨터나 네트워크의 자원에 대한 접근이 막히거나, 성능이 떨어질 때 발생되는 것이다. 이러한 공격은 직접적으로 또는 영구적으로 데이터에 손상을 주지 않을 수도 있지만, 그들은 의도적으로 자원의 가용성을 조작할 수 있다. 공격자들은 공유자원을 모두 소모하여 다른 사용자들이 사용할 공유자원이 남아있지 않게 하거나, 자원들의 질을 떨어뜨려 사용자들이 사용하기에 더 이상 가치가 없게 만드는 등의 자원을 작동 불능하게 만들어 DoS 공격을 수행한다.

2.1 DoS 공격 유형의 분석

DoS 공격은 공격자가 시스템의 취약점을 찾아내기 위한 도구를 사용하면서 시작된다. 다음엔, 적당한 프로세스나 프로세스 그룹에 대한 인증되지 않은 접근 권한 및 방법으로 프로세스를 사용하게 된다. 그리고 나서 공격자는 파일을 파괴하거나, 프로세스의 성능을 떨어뜨리거나, 남은 저장 용량을 고갈시키고, 프로세스나 시스템을 정지시킴으로 DoS 공격을 완수한다.

2.2 DoS 공격 유형 분류 체계

서비스 거부 공격 방법은 크게 두 가지로 분류될 수 있다[2, 3]. 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 유형인 일반적인 분류 체계와, 시스템의 취약성을 기반으로 하는 분류 체계로 구분된다.

2.2.1 일반적인 분류

시스템 내부에서 행해지는 서비스 거부 공격은 일반적으로 다음과 같이 4가지로 분류된다.

(1) 파 괴

공격자는 사용자나 호스트 또는 시스템에 접근 권한을 얻어, 중요한 시스템 파일들의 일부 혹은 전부를 삭제하거나 변조시킨다.

(2) 프로세스 성능 저하

시스템 내 프로세스들의 오버로딩(overloading)을 야기하는 공격이다. 이렇게 되면, 성능저하나 오동작으로 인해 해당 프로세스에 할당되어 있던 자원의 질이 떨어지게 되고 이러한 자원을 사용하는 사용자에게 올바른 서비스나 접근을 거부하게 하는 공격이다.

(3) 디스크 자원 고갈

목표 호스트나 네트워크에 디스크 제한 용량을 가득 채우거나 사용자의 가용공간을 소모하는 것을 목적으로 하는 공격이다.

(4) 가동정지(종료)

공격자는 시스템에서 수행중인 하나이상의 프로세스를 정지시키거나 시스템을 종료하는데 목표를 두고 있다.

2.2.2 취약성에 의한 분류

본 논문의 기초 자료 조사를 위해 이용된 사이트인 securityfocus.com[9]에서 분류하고 있는 취약성 기준은 9개의 범주로 구분되고 있으며 그 내용을 요약하면 <표 1>과 같다.

〈표 1〉 취약성 분류 기준

범 주	발 생 원 인
경계조건 에러	· 가용한 어드레스 영역을 벗어나 읽기/쓰기 시도 · 시스템 자원의 고갈 · 고정-크기 데이터 구조의 오버플로우
액세스 검증에러	· 주체가 액세스 도메인 객체 외부에 오퍼레이션을 실시하도록 제기 · 주체의 액세스 도메인 외부 디바이스나 파일에 읽기/쓰기의 결과 · 객체가 인가되지 않은 주체로부터의 입력을 수용 · 시스템의 주체를 적절히, 완벽히 인증하지 못함
입력검증 에러	· 프로그램이 문장 구성상 부정확한 입력의 인식 실패 · 모듈이 관계 입력 필드를 받아드릴 때 · 없어진 입력 필드를 처리할 때 · 필드-값의 상호관계 에러
예외적인 상태처리 실패	· 시스템이 기능적 모듈, 디바이스, 또는 사용자 입력에 의해 생성되는 예외적인 상태를 적절히 처리하지 못함
경합조건 에러	· 두 오퍼레이션간 타이밍 윈도우 동안 나타나는 에러
연속에러	· 부적절하거나 부적당한 오퍼레이션의 연속 제기
원자수 에러	· 부분 수정된 데이터 구조가 다른 프로세스에 의해 관찰 · 원자를 가져야만 하는 일부 오퍼레이션이 부분적으로만 수정된 데이터를 가지고 중단된 코드 때문에 발생
환경에러	· 기능적으로 정확한 모듈사이의 특정 환경에서 상호작용으로 기인 · 프로그램이 특정 머신, 특별한 구성 하에서 수행될 때 발생되는 에러 · 운영 환경이 어떤 것을 위해 설계된 소프트웨어와 차이가 때문에 발생
구성에러	· 시스템 유틸리티가 부정확한 설정 매개변수를 가지고 설치 · 액세스 퍼미션이 시큐리티 정책을 위반할 수 있도록 유틸리티에 부정확한 설정

2.3 기존 분류체계의 한계점

기존의 일반적인 DoS의 분류체계는 공격자의 행위와 공격의 영향으로 단순히 시스템에 어떠한 영향을 미치는가에 대한 결과를 위주로한 분류였다. 이러한 일반적인 분류는 잠재적인 취약성을 분석하여 문제점을 미연에 방지하거나 이러한 문제점의 해결방법을 모색하고 관련 버그를 수정 개선하는데 활용하기에는 좋은 방법이지만 실시간적으로 공격의 가능성과 공격의 유무를 파악하는 침입탐지에서는 적절한 분류방법이 되지 못한다.

〈표 2〉 성능 메트릭 변수

유 형	종 류
파일시스템 정보변수	FS % Used, FS KBytes Used, FS KBytes Free, FS KNodes Used, FS KNodes Free, FS Frag Size
프로세스 정보변수	Procs Total, Procs In Core, Procs In Sleep, Procs In Run, Procs In Idle, Procs In Zombie, Procs In Stop, Procs In Other, Procs % Used
원격활동 변수	Phus Read, DIS Msg Recv,Phys Write, PFS Msg Recv, Log Read, read Cache Flush, Log Write, Inval Cache Flush, DIS Msg Sent, Cache Flush, RFS Msg Sent
네임케쉬 변수	Name Cache Size, Name Cache % Hits, Name Cache Misses, Name Cache Long Enter, Name Cache Lru Empty, Name Cache Enters, Name Cache Dir Scans, Inode Gets, Dir Blks Read, Name Cache Access Name Cache Mv to Front
RPC 관련변수	RPC Client Calls, RPC Server Calls, RPC Client Badcalls, RPC Server Badcalls, RPC Client Retrans, RPC Server Retrans, RPC Client Badxids, RPC Server Badxids, RPC Client Timeouts, RPC Server Timeouts, RPC Client Wait, RPC Server Wait, RPC Client Newcred, RPC Server Newcreds, RPC Client Timers, RPC Server Timers, RPC Client No Mem,
원격 시스템 호출변수	Syscalls_In, Sysexecs In, Syscalls Out, Sysexecs Out, Sysreads In, Chars Read In, Sysreads Out, Chars Read Out, Syswrites In, Chars Write In, Syswrites Out, Chars Write Out, Sysforks In, Sysforks Out
시스템 호출 변수	KChars Read, KChars Write, Syscalls, Sysreads, Syswrites, Sysforks, Sysexecs, Device Intrps, FP Intrps, Contx Swtch

3. DoS 공격 유형 분류체계 제안

DoS 공격의 형태는 아주 다양하게 일어난다. 앞장에 제시된 일반적인 분류방법은 실제로 침입 탐지 시스템을 구현하기에는 부적당하다. 이유는 실시간적인 침입탐지 능력을 보유하기 위해서는 징후를 감지하고 그 징후에 따른 탐지 전략이 수립될 수 있어야 하며, 어떠한 징후에 따른 관찰 대상이 무엇인지를 분명히 할 수 있도록 해야한다. 이는 if then 규칙을 적절히 활용할 수 있으며, 관련 유형을 체계적으로 분류함으로서 공격의 특징을 추출하는데 많은 도움을 준다.

따라서 이 분류법에서는 구동 시스템에서 공격 대상을 기반으로 하는 공격 요소의 직접적인 특성화를 제안한다. 추상적 분류 계층구조는 카테고리 내에 표현될 수 있는 시그네쳐와 관련해서 하위 카테고리를 포함하는 상위 레벨에서의 카테고리인 4개의 카테고리로 구분한다. 각 카테고리에 부합되는 명확한 경계는 이

추상적인 카테고리를 설명함으로서 만들어질 수 있고, 실례는 C2 레벨 감사 추적 이벤트에 관련한 상위 레벨 이벤트 구조의 명확한 정의를 요구한다. 예로서 계층 구조의 간단한 실제 예는 감사 추적 이벤트를 정의함으로서 만들어진다. 여기서 하위 레벨 감사 추적 이벤트는 공격대상 분류 즉 상위 레벨에 속하는 성능 메트릭의 클래스가 된다.

이것은 계층구조의 여러 카테고리에서 침입 시그네쳐의 특별한 분포를 가져온다. 그러한 정의의 최선의 선택은 감사 추적의 특징에 의존하게 되며, <표 2>와 같은 성능 메트릭 변수를 활용하여 DoS 공격 탐지 시스템을 효율적으로 설계할 수 있는 다음과 같은 분류 체계를 제안한다.

3.1 비휘발성 자원 고갈 공격

비휘발성 자원이라 함은 디스크 공간, I-node 수, 임시 파일 수, 프로세스 생성 수 등 자원의 한계가 변화지 않는 자원을 의미하며, 취약성 분류법의 경계조건에러가 이러한 자원의 한계점을 이용한 공격에 속할 수 있다. 디스크는 제한된 용량을 가지고 있기 때문에 공격자가 사용자의 디스크 제한 용량(quota)을 가득 채운다면, 해당 사용자나 전체 호스트는 "disk full" 조건이 바뀌기 전까지는 사용할 수가 없게 된다. 이러한 공격에는 "메일 폭탄"나 "메일 스팸" 같은 것들이 있다.

또한, 디스크나 네트워크 파일 시스템에 파일시스템의 I-node 용량을 넘어서게 하는 많은 양의 빈 파일들을 만드는 방법이 있다. I-node는 각 파일의 디스크상의 주소와 여러 속성을 담고 있는 파일과 연관된 특별한 테이블로서 작은 파일일 경우에는 I-node와 해당 파일이 함께 저장되고, 큰 파일일 경우에는, I-node는 실제 파일이 저장된 디스크상의 주소를 가리키는 포인터를 가지고 있다. 만일, 가용한 I-node가 모두 소비된다면, 운영체제는 가용한 디스크 공간이 남아있다고 해도 새로운 파일을 생성할 수 없게된다.

3.2 휘발성 자원 고갈(과부하) 공격

이는 시스템의 처리 능력에 기인하는 것으로 호스트 컴퓨터의 프로세스들이 오버로딩되면, 성능저하나 사용할 수 없게된 자원에 의해 그 자원을 사용하는 프로세스들의 처리능력이 떨어지게 된다. 이는 공격자가 인터넷을 통해 호스트에 연결하고, 개인사용자나 전체 호스트에 대해 해당 호스트가 더 이상 감당할 수 없을 때까지 새로운 프로세스를 생성하게 되는데, 이러한 일을 가능하게 하는 프로그램을 흔히 "fork bombs"라고 한다.

또한, CPU의 오버로드를 야기하면서 CPU의 많은 시간을 소모하는 많은 프로세스를 생성해 호스트 컴퓨터를 매우 느리게 하는 것이다. 대표적인 네트워크 서비스에 기반한 네트워크 공격 유형 중 하나가 "브로드케스트 스톰"으로서, 호스트가 방송패킷을 받게 되면, 응답을 해야 할지를 결정하고, 목적지 주소로 응답을 돌려보내는데, 이는 또 다른 방송 패킷을 발생시킨다. 몇몇의 호스트가 서로 방송 패킷을 무한히 주고받게 되면, 이는 결국 전체적인 네트워크를 마비시킨다.

3.3 프로세스 공격

이 공격은 직접적으로 호스트 컴퓨터의 명령어 인터페이스에 접속하여 시스템 프로세스, 데몬 프로세스와 같은 프로세스를 공격하는 "시스템 응용" 공격과, 인터넷 프로토콜 스위트인 TCP/IP 계층에 따른 분류에서 애플리케이션 층에 해당되는 HTTP, FTP, Telnet, SMTP 등의 프로세스에 대한 공격인 "네트워크 응용" 공격으로 분류될 수 있다. 이들 공격 형태는 공격자가 호스트나 네트워크의 하나 또는 그 이상의 프로세스를 정지시키는데 목표를 두고 있다. 만일 공격자가 접근 권한을 가지고 있다면, 프로세스를 죽이거나 시스템을 완전히 종료시키는 적당한 명령어를 사용하여 목적을 달성할 수 있다. 유닉스에서의 "kill" 명령은 프로세스를 종료시키는데 사용할 수 있는 명령어의 한 예이다.

3.4 파일 시스템 공격

만일, 공격자가 사용자나 호스트 또는 네트워크에 접근 권한을 얻는다면, 공격자는 데이터 생성, 변조, 삭제 공격을 통하여 파일들의 일부 혹은 전부를 삭제하거나 붕괴시킬 수 있고 이 파일의 사용자들에 대해 사용 거부를 할 수 있다. 또한 네트워크 파일들이 파괴되면, 네트워크을 통한 서비스가 질이 떨어지거나 사용할 수 없게 된다.

컴퓨터 바이러스나, 웜은 시스템 파일의 일부 혹은 전부를 붕괴시킬 수 있는 부분을 포함하고 있다. 그리고 인터넷에서 사용되는 talk나 E-Mail과 같은 "flash family"에 의해서 또 다른 방법으로도 공격이 행해진다.

3.5 기타 공격

기타 공격은 위의 범주에 속하지 않거나 새롭게 제시되는 공격에 대한 명확한 유형이 분석되지 않았을 경우 임시로 분류한다.

4. 제안된 방법의 분류 검증

분류 체계에 대한 명확한 검증 지침은 알려져 있지 않지만 다음과 같은 몇 가지 기준을 가지고 제시된 분류 체계를 조명해 본다.

4.1 상호배타성 & 명백성

이 특성은, 분류의 각 부문은 한 부문의 분류 기준이 다른 부문의 분류 기준을 포함해서는 안되며 그 기준이 명확해야 한다는 것이다.

제안된 분류 체계는 각 분류 항목이 공격자체를 대상으로 한 것이 아니라, 목표를 대상으로 하여 분류하였고, 이 공격 목표는 시스템 자원들로서 서로간에 쉽게 구별된다.

4.2 완전성

완전성은 분류의 모든 부문들이 모든 가능성을 포함해야 한다는 것이다. 제안하는 분류체계는 securityfocus.com에서 제공하고 있는 데이터베이스에서 현재(1999.7)까지의 DoS 공격중 모든 가능한 공격 목표를 고려하여 <표 3>과 같이 완벽히 분류될 수 있음을 제시하였다.

4.3 수용성 & 유용성

수용성은 분류의 각 부문은 논리적이고 직관적이어서 쉽게 납득이 되어야 한다는 것이고, 유용성은 실제 활용시에 통찰력 있는 정보를 줄 수 있어야 한다는 것이다.

제안한 분류는 직관적으로 알 수 있도록 논리적인 과정을 기반으로 했으며, 향후 성능 시그네처를 이용한 서비스 거부 공격 침입탐지 설계를 위한 첫단계로서 성능 감시에 효율적인 방안으로 제시된 것이다.

4.4 적용분석

이 사이트에서 분류하고 있는 취약성 분류체계에 따른 DoS 공격의 유형을 살펴보면 <표 1>를 기준으로 경계 조건 에러, 예외적인 상태 처리 실패, 설계 에러, 입력 검증 에러, 액세스 검증 에러의 순으로 조사되었으며, 환경 에러와 구성 에러는 각각 1건씩 조사되었다. 그리고 원인이 알려지지 않았거나 취약성 범주에 속하지 못한 공격 유형이 8건이나 되는 것을 알 수 있다. 이러한 분류 체계는 DoS 공격에 대해 특성화 한 것이 아니기 때문에 새롭게 나타나는 공격 방법들이 DoS 공격을 적절히 분류하지 못함을 의미한다.

〈표 3〉 DoS 공격 유형의 분류

제안된 DoS공격분류	대상자료 건수	취약성 분류기준
비휘발성 자원고갈공격	1	Design Error
	1	Failure to Handle Exceptional Conditions
	1	Configuration Error
	1	Unknown
부하공격	3	Design Error
	2	Boundary Condition Error
	2	Input Validation Error
	1	Failure to Handle Exceptional Conditions
	1	Configuration Error
파일시스템 공격	1	Design Error
	1	Input Validation Error
	1	Configuration Error
	2	Unknown
프로세스공격	1	Design Error
	3	Boundary Condition Error
	2	Access Validation Error
	1	Input Validation Error
	10	Failure to Handle Exceptional Conditions
	1	Environment Error
	5	Unknown

<표 3>은 새로이 제시된 분류법에 취약성을 기준으로 한 분류법에 따라 분류한 결과를 재분류한 것이다. 이 결과 41건의 DoS 공격 취약성 중 비휘발성 자원고갈 공격에 4건, 부하공격에 9건, 프로세스 공격 23건, 그리고 파일 시스템 공격에 5건이 분포됨을 알 수 있다. 이중 프로세스 공격의 유형 건수를 살펴보면 데몬 프로세스 공격에 12건, 일반프로세스 공격에 4건 그리고 시스템 프로세스 공격에 7건으로 가장 많은 공격이 이루어짐을 알 수 있다.

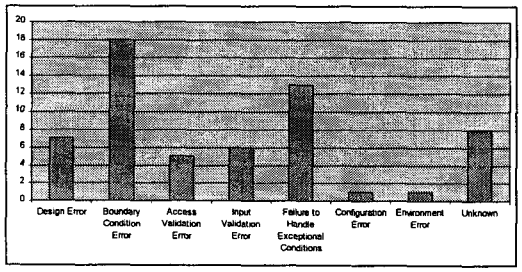
이를 기존의 분류체계와 제안된 분류체계를 비교한 분류 분포도는 (그림 1, 2)와 같다.

본 분류법은 기존의 일반적인 분류체계의 한계점을 DoS 공격의 특성에 맞게 극복하고 계층화 구조로 조직화 할 수 있도록 하였으며, 다음과 같은 특성을 지닌다.

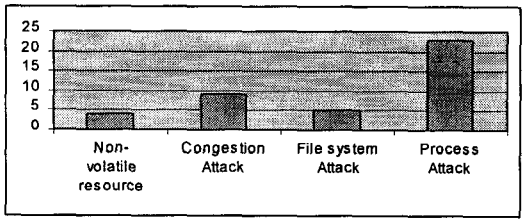
- 침입 시그네처의 카테고리화를 허용하며, 매칭의

기본이 되는 계산적 틀 구조와는 독립적

- 계산적 틀 구조를 초기화하는 기본으로 제공
- 각 카테고리는 독립적으로 취급될 수 있으며, 계산적 절차는 그 카테고리 내에서 시그네쳐를 일치시킬 수 있음
- 매칭 문제에서 본질적으로 다른 해결방법 허용
- 단일화된 절차는 모든 카테고리가 표현되고 하나의 모델에 일치되도록 고안될 수 있음



(그림 1) 취약성에 따른 분포도

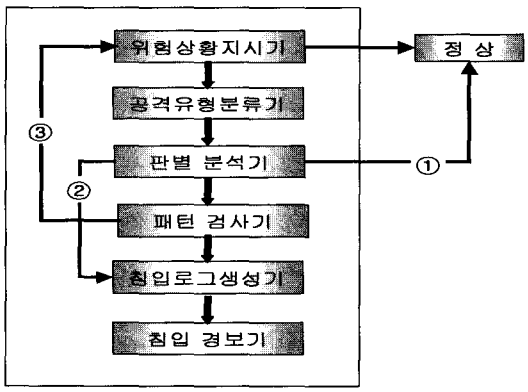


(그림 2) DoS 공격 유형에 따른 분포

4.5 새로운 분류법에 의한 침입 탐지 모듈 구조

제시된 분류법은 (그림 3)의 침입탐지 시스템 모듈을 갖는 IDPS 설계를 위한 기반 단계로서 실제적으로 어떻게 적용되는가에 대해 소개한다. 여기서 공격유형 분류기는 공격에 대한 관찰대상을 감지하고 있어 위험상황을 지시 받으면 새롭게 제시한 분류법을 가지고 5가지 공격유형 중 하나를 판별하게 된다.

판별 분석기는 각 공격별 시뮬레이션을 통해 얻어진 분석식을 가지고 공격의 유무를 판별하게 되는데 ①은 분석식에 의해 계산된 값이 일정범위 이하일 경우 공격이 아님을 판별하게 되고 ②는 일정 범위 이상일 경우에 패턴검사 없이 바로 침입로그를 생성하게 된다. 계산 값이 일정 범위 내에 있을 경우 패턴검사기에 의해 다시 상세 검사를 하여 침입 여부를 판단하게된다. ③의 경우는 공격의 징후가 있으면서도 패턴 검사기로도 정확히 판별이 안될 경우 다시 감시 대상이 되어



(그림 3) 침입탐지 시스템 모듈

다시 위의 사이클을 반복하게 된다.

5. 결 론

본 논문에서는 향후 IDPS 설계를 목표로 이에 합당한 새로운 서비스 거부 공격에 대한 분류 체계를 제안하였다. 기존의 분류체계가 제시하는 DoS분류유형은 새롭게 나타나는 공격방법과 지능적으로 공격패턴을 달리하는 공격방법들을 적절히 분류하지 못하는 한계를 가지고 있고 너무 세밀한 분류로 인하여 실시간적으로 침입탐지를 위한 분류방법으로는 적절치 못하였다.

본 논문에서 제시하는 DoS공격에 대한 새로운 분류는 침입패턴을 효과적으로 감지하고 실시간적으로 탐지의 효율성을 증대시키기 위한 분류체계를 확립하고자함에 그 목적이 있다. 제시한 분류체계는 공격유형이 시스템에 어떠한 징후와 결과를 주는가 그리고 DoS공격 침입 탐지 모델특성에 중점을 두어 공격의 유형을 휘발성 자원 고갈 공격, 부하공격(휘발성공격), 프로세스공격, 파일 시스템 공격으로 4가지 범주로 새로이 구분을 하였다. 이는 공격유형이 어떠한 범주에 속하는지 정확히 판단, 확인하여 분류 속성에 따른 실시간적인 침입탐지 알고리즘을 개발하는데 활용할 수 있다.

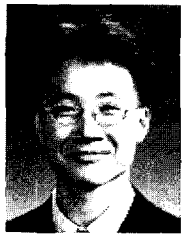
참 고 문 헌

[1] Mandy Chung, Nicholas Puketza, Ronald A. Olsson, "Simulating Concurrent Intrusions for Testing Intrusion Detection Systems : Paralleli-

zing Intrusions," Proc., 18th National Information Systems Security conference, Baltimore, MD, pp.173-183, October 1997.
[2] Herve Debar, Marc Dacier and Andres Wespi, "Towards a Taxonomy of Intrusion Detection Systems," Research Report of IBM Research Division, Zurich Research Laboratory, Jen. 1998
[3] Taimur Aslam, Invan Krsul and Eugene Spafford, "Use of A Taxonomy of Security Faults," In 19th National Information System Security Conference Proceedings, Baltimore, MD, Oct. 1996
[4] T. Lane and C. E. Broadly, "An application of machine learning to anomaly detection," Proc. of NISSC'97, pp.366-380, 1997.
[5] Brian Marick. "A survey of software fault surveys," Technical Report UIUCDCS-R-90-1651, University of Illinois at Urbana Champaign, December 1990.
[6] Richard A. DeMillo, W. Michael McCracken, R. J. Martin, and John F. Passafiume. "Software Testing and Evaluation," The Benjamin/Cummings Publishing Company Inc., 1987.
[7] N. Puketza, B. Mukherjee, R. A. Olsson, and K. Zhang, "Testing Intrusion Detection Systems : Design Methodologies and Results from an Early Prototype," Proc. 17th National Computer Security Conference, Vol.1, pp.1-10, October 1994.
[8] A. K. Ghosh, A. Schwartzbard and M. Schatz, "Learning program behavior profiles for intrusion detection," Proc. of WIDNM '99, 1999.
[9] http://www.securityfocus.com/vdb
[10] 김광득, 이상호, 성능 시그네쳐를 이용한 서비스 거부 공격 침입탐지 시스템 설계, 정보처리학회 '99 춘계 학술발표 논문집, pp.816-819, 1999.

김 광 득

e-mail : kdkim@kier.re.kr
1987년 대전산업대학교 전자계산학과 졸업(공학사)
1989년 전북대학교 대학원 전산통계학과 졸업(이학석사)
1994년~현재 충북대학교 대학원 전자계산학과 박사과정 수료
1981년~현재 한국에너지기술연구소 선임기술원
관심분야 : 컴퓨터 보안, 침입탐지 시스템, 네트워크 관리 등



박 승 균

e-mail : webbian@cnlab.chungbuk.ac.kr
1998년 충북대학교 통계학과 졸업(이학사)
1999년~현재 충북대학교 대학원 컴퓨터 과학과 석사과정
관심분야 : 컴퓨터 보안, 침입탐지 시스템, 네트워크 프로그래밍 등

이 태 훈

e-mail : hoon2002@cnlab.chungbuk.ac.kr
1999년 충북대학교 임학과 졸업(농학사)
1999년~현재 충북대학교 대학원 컴퓨터과학과 석사과정
관심분야 : 컴퓨터 보안, 침입탐지 시스템 등

이 상 호

e-mail : shlee@cbucc.chungbuk.ac.kr
1976년 숭실대학교 전자계산학과 졸업(공학사)
1981년 숭실대학교 대학원 전자계산학과 졸업(공학석사)
1989년 숭실대학교 대학원 전자계산학과 졸업(공학박사)
1976년~1979년 한국전력 전자계산소 프로그래머
1981년~1983년 한국전자통신연구소 위촉연구원
1990년~1991년 호주 텔레콤 연구소 방문연구원
1992년~1993년 캐나다 UBC 방문연구원
1981년~현재 충북대학교 컴퓨터과학과 교수
관심분야 : Protocol Engineering, Network Security, Network Management, Network Architecture 등