네트워크 기반 프로토콜 공격에 대한 침입탐지 시스템의 설계

최준욱 °, 이정준, 정운영, 정선화, 박석천
경원대학교 컴퓨터공학과
{jjoonyya °, mrcool, woon0, smw0}@comnet.kyungwon.ac.kr, scpark@kyungwon.ac.kr

Design of Network-based Intrusion Detection System for Protocol Attack

Joon Wook Choi °, Jeong-Jun Lee, Woon Young Jung, Sun-hwa Jung, Seok-Cheon Park
Dept. of Computer Engineering, Kyungwon University

요 약

DOS (Denial Of Service)에 대한 공격은 시스템의 정상적인 동작을 방해하여 시스템 사용자에 대한 서비스 제공을 거부하도록 만드는 공격으로 현재 이의 공격에 대한 탐지 알고리즘 및 연구들이 많이 제시되고 있다. 본 논문에서는 네트워크 또는 트랜스포트 계층에 해당하는 프로토콜(TCP/IP, ICMP, UDP) 공격을 분석하고 이들 프로토콜의 취약점을 공격하는 DOS 공격 이외의 다른 공격을 탐지하기 위하여 프로토콜의 기능별, 계층별에 따른 모듈화 작업을 통하여 네트워크 침입탐지 시스템을 설계하였다.

1. 서 론

초기 연구와 군사 목적으로 발전한 인터넷은 인터넷의 확산과 분산 컴퓨팅 환경의 발달로 원격 접속의 컴퓨터 사용이 증가하면서 다양한 인터넷 프로토콜과 이를 기반으로한 인터넷 서비스들이 확장되고 있다. 이와 함께 역기능들이 날로 증가되고 있으며 그 피해 규모 또한 심각한 수준에 이르고 있다. 현재 이에 대한 많은 연구가 진행중이지만 대부분의 연구용 침입탐지 시스템은 관리상의 불편 및 탐지 규칙의 부족 등으로 인해 실제 환경에서 적용하기에는 힘든 단점을 가지고 있다. 최근 사용되는 네트워크 공격 방법으로는 미국의 대표적 웹 사이트들을 무차별하게 공격할 때 사용되었던 방법인 서비스 거부 공격(DOS : Denial of Service Attack)이 많이 사용되고 있다. 현재 이러한 서비스 공격에 대해서는 많은 연구가 이루어지고 있지만 서비스 거부 공격 방식을 자세히 살펴보면 전체적으로 프로토콜의 취약점을 공격한 방법들 중의 일부분으로 볼 수 있다. 따라서 본 논문에서는 기존에 널리 알려진 이러한 서비스 거부 공격(DOS) 뿐만 아니라 네트워크 프로토콜의 취약성을 공격하는 행위에 대해 리눅스 상에서 네트워크 패킷을 분석하고 각 프로토콜에 해당하는 침입들을 탐지하여 프로토콜별 공격 유형들을 탐지 할 수 있는 네트워크 기반 침입탐지 시스템을 설계하였다.

2. 네트워크 기반 침입탐지 시스템의 구성

네트워크에 흐르는 패킷을 감시함으로써 침입을 감시하는 시스템을 네트워크 기반 침입탐지 시스템이라 하고 기능을 살펴보면 다음과 같다. 분석 측면에 있어서 패킷을 분석하는 모듈은 필터링을 수행하는 시스템에 따라 달라질 수 있다. 만약 일반 패킷 필터링 수준의 시스템이면 BPF 드라이버를 통해 들어오는 패킷들을 프로토콜별로 헤더를 분석하여 관리자에게 알려줄 것이며, 어플리케이션 수준의 모니터링 시스템이면 이러한 패킷들을 모아서 보다 복잡한 정보를 생성하고 분석하여 각 프로토콜별 침입에 대한 탐지를 한다. 그리고 분석한 패킷이나 모아진 어플리케이션의 정보를 나중에 이용하기 위해서는 적절한 형태로 변형되어 데이터베이스에 기록을 해두고 다음 공격에 대비한다. 이러한 네트워크에서 패킷의 효율적인 처리를 위해 제안한 침입탐지 시스템의 구성은 그림 1과 같다.

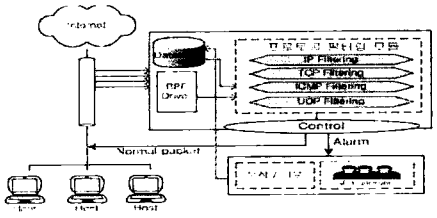

그림 1 침입탐지 시스템 구성도

3. 침입탐지 시스템의 프로토콜 공격 탐지

프로토콜별 공격에 대해서 패킷들을 탐지하기 위해서는 네트워크상의 패킷을 실시간으로 수집하고 프로토콜을 분석하여 수

락 여부를 결정하는 기술이 필요하다. 본 논문에서 제안한 침입 탐지 시스템은 내부 네트워크로 들어오는 이더넷(Ethernet 10Base_T) 데이터에 대해 작동 하여 데이터 패킷은 frame 형태로 전송한다. 링크계층을 구성하는 인터페이스의 특성에 따라 이더넷에서 제공하는 MTU 1500 바이트 패킷을 필터링하고 BPF 드라이버를 이용해서 침입 탐지 시스템을 구성하였다. 전체적인 프로토콜 공격 탐지는 표 1과 같은 방법을 통해서 탐지가 가능하다.

표 1 공격 유형에 따른 프로토콜 공격 탐지

공격 유형별 탐지 방법	프로토콜 공격 유형
Source/Destination address filtering	IP Spoofing Attack, LAND Attack
Port filtering	IP Spoofing Attack(21 Port), LAND Attack(139 Port), UDP packet storm Attack(7 port, 19 Port) , IP Fragemtn(specific port), SYN Flooding (specific port)
Over size filtering	IP Fragment Attack
Buffer overflow filtering	SYN Flooding Attack
Traffic counting filtering	Smurf Attack, Trinoo Attack, SYN Flooding Attack

4. 프로토콜 공격에 대한 침입탐지 시스템의 설계

프로토콜 공격에 대한 침입탐지 시스템을 설계하기 위한 각 모듈들은 아래와 같다.

(1) 패킷 캡쳐 모듈

패킷을 캡쳐하기 위해서 리눅스에서 기본적으로 제공하고 있는 BPF 드라이버를 이용한다. 아래 그림 2는 BPF 패킷 캡쳐 드라이버를 나타낸 것이다.

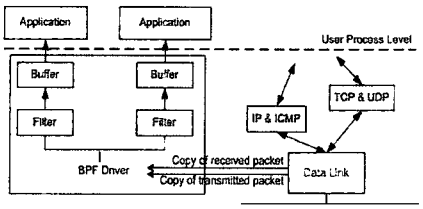

그림 2 BPF 패킷 캡쳐 드라이버

패킷이 네트워크 인터페이스로 도착되면 데이터링크 레벨 디바이스 드라이버는 시스템 프로토콜 스택을 BPF 드라이버로 보내고, 만약 드라이버가 인터페이스를 읽고 있는 중이라면 드라이버의 첫 번째로 네트워크 탭을 호출한다. 사용자 정의 필터는 패킷을 받아들일지 또는 얼마나 많은 바이트의 패킷을 저장할지를 결정하게 되며 필터링 과정을 거쳐 응용 레벨로 전달한다. 어플리케이션은 한번에 하나 이상의 패킷을 받을 수 있는데 이러한 경우 드라이버는 각각의 프로세스가 요구하는 필터들을 모두 고려하여 패킷을 처리한다. 이러한 방법으로 드라이버는 커널 레벨에서 시스템의 성능을 크게 저하시키지 않고 패킷을 캡처링 할 수 있다.

(2) 패킷 필터 모듈

리눅스에서는 침입을 탐지하기 위한 이전 단계로 사용자 레벨에서 패킷을 필터링하기 위해서 libpcap 라이브러리에서 제공하고 있는 함수를 이용한다. BPF 드라이버에서 캡처링한 패킷들을 사용자 레벨에서 적절하게 필터링을 하기 위해 그 과정을 순서도로 나타내면 그림 3과 같다.

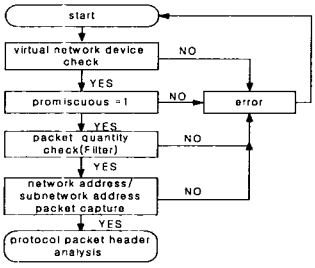

그림 3 패킷 필터링 과정

패킷 필터링 모듈에서 이용한 함수는 다음과 같다.

- pcap_lookupdev() 함수는 BSD 계열의 네트웍 디바이스를 가져오는 함수이다.
- pcap_open_live() 함수는 실제 디바이스의 기기를 열어주는 함수이다. 설정되는 파라매터를 통해서 수집할 패킷의 길이를 결정하며 promiscuous를 1로 설정하면 모든 패킷을 받아들일 수 있다.
- pcap_snapshot() 함수는 위의 파라매터에서 정의한 snapshot를 가상 디바이스에 세팅을 한다.
- pcap_lookupnet() 함수는 열려진 캡쳐 드라이버에 네트워크 주소와 서브넷 주소를 넘겨준다.
- pcap_compile() 함수는 패킷 필터를 컴파일 한다.
- pcap_setfilter() 함수는 컴파일 된 필터 프로그램을 패킷 캡쳐 디바이스로 읽어들인다.
- pcap_loop() 함수는 packet count의 수만큼 패킷을 캡쳐해서 printer가 지정하는 함수를 수행한다.

이러한 함수를 사용함으로써 가상 디바이스로 패킷들을 수집하고 필터링 룰에 의해 관리자가 원하는 패킷만을 얻을 수 있다.

(3) 프로토콜별 침입탐지 모듈

적절하게 필터링된 패킷들은 프로토콜이 가지는 취약점의 분석을 위해서 프로토콜을 IP, TCP, UDP, ICMP의 단계 별로 헤더 정보를 분석하였다.

그림 4는 프로토콜별 침입탐지 모듈에 대한 그림이다.

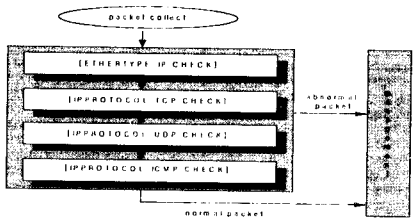

그림 4 프로토콜별 침입탐지 모듈

분류된 프로토콜들은 그들이 가지는 패킷의 특정 옵션 필드나 타입을 추출하는 과정을 시작으로 헤더의 필드에 해당하는 지정된 값을 통해 취약성을 분석하고 탐지 및 필터링함으로써, 실시간으로 각 프로토콜에 해당하는 공격을 탐지하며 마지막으로 비정상적인 패킷이 아님을 판정하기까지의 과정을 IP, TCP, UDP, ICMP 프로토콜별로 모듈화 하였다. 이는 기존의 서비스 거부 공격 탐지 방법들을 프로토콜별로 공격을 탐지할 수 있도록 재분류한 침입탐지 모듈이며 또한 fragment 공격과 포트 공격에 대한 탐지 기능 모듈을 추가하여 탐지 능력을 향상시켰다. 그림 5는 프로토콜별 침입탐지 시스템에 대한 알고리즘이다.

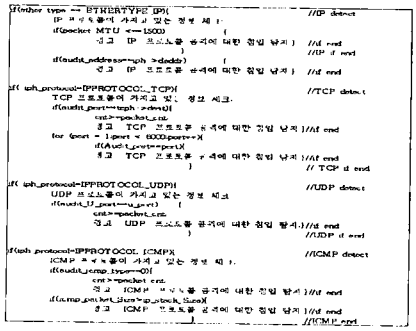

그림 5 프로토콜별 침입탐지 알고리즘

(4) 프로토콜별 침입탐지 시스템의 동작 절차

본 논문에서는 DOS에 의한 서비스 거부 공격 및 그 외의 프로토콜의 취약점을 이용한 공격을 탐지하기 위해 Ethernet 상에서 들어오는 네트워크 패킷의 정보를 프로토콜별 침입탐지 모듈을 통해서 프로토콜별 분석 과정을 거친 후 정상/비정상 패킷임을 탐지하여 비정상 패킷을 탐지하면 관리자에게 통보하여 공격 사실을 보고하도록 하였다. 본 논문에서 설계한 프로토콜별 침입탐지 시스템 기능부의 동작 절차는 그림 6과 같다.

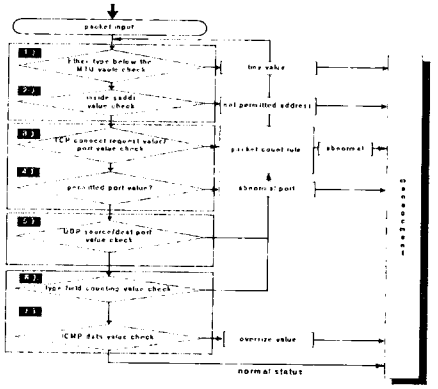

그림 6 침입탐지 시스템 기능부의 동작 절차

5. 결 론

본 논문에서는 침입탐지 시스템의 설계를 위해서 패킷 수집 및 침입탐지 모듈을 이용하여 프로토콜별로 공격의 유형을 분류하고 침입의 특성을 분석하여 기존의 서비스 거부 공격을 위한 탐지 알고리즘이 갖는 한계점을 보완한 확장된 침입탐지 알고리즘을 제안하였으며, 침입탐지 시스템의 동작 절차를 토대로 프로토콜별 침입탐지 시스템을 설계하였다.

DOS 공격에 대한 해결 방법 및 알고리즘은 많이 제안 되어있지만 본 논문에서는 DOS 공격을 프로토콜의 각각에 해당하는 공격으로 포함시켜 놓고 그 외에 발생되는 침입을 프로토콜별로 모듈화 하여 설계하였다.

참고문헌

[1] Infomation Security, Dept. of Math. Inha Univ, 1999-2000.
[2] http://ns.certcc.or.kr
[3] Security+ For UNIX,The Pohang University of Science and Technology, February,1997.
[4] An Approach for TCP Connection Hijaking Attack D.H.Kim, S.I.Park, Y.s.Sek, K.s.Park, J,Y,Lee Dapartment of Computer Engineering, Hallym, University.
[5] 윈도우 시스템에 대한 원격 서비스 거부 공격(DOS)과 대책,1998. 06. 한국정보보호센터 기술본부 기술대응팀.
[6] UNIX network programing Networking APIs:socket and XTI,W.RICHARD STEVENS,1998.
[7] 윈도우시스템 서비스 거부공격과 대책, 1998, 한국정보보호센터 기술본부