

IDS 우회공격 탐지 시스템 설계 및 구현

길 민 육**, 차 준 남*, 이 극*

*한남대학교 정보통신멀티미디어학부

**문경대학교 인터넷정보계열

요 약

우회공격 기술이란 침입탐지 시스템의 취약점을 이용하여 정상적인 침입탐지를 회피하는 기술이다. 본 논문에서는 첫째, 침입탐지 시스템에 대한 우회공격 기술을 분류하고, 두 번째로 기존의 침입탐지 시스템에서 사용할 수 있는 우회공격 탐지 모델을 제시하고 마지막으로 우회공격 탐지 시스템을 설계 구현한다.

A Design and Implementation of Detection System against Evasional Attack to IDS

Min-Wook Kil**, Jun-Nam Cha*, Geuk Lee*

ABSTRACT

IDS(Intrusion Detection System) evasion is a technology which uses vulnerability of IDS in order not to be detected by IDS. In this paper, at first, we classify IDS evasion technology. Second, we propose detection model of IDS evasion technology. Finally, we design and implement detection system of IDS evasion.

1. 서 론

최근 정보통신 기술의 발전과 현대의 정보화 지향적인 흐름에 힘입어 인터넷을 통한 전자상 거래, 홈뱅킹 등 네트워크를 이용한 새로운 서비스들이 다양하게 개발되어 사용자가 크게 증가되고, 인트라넷 구축을 통한 공, 사기업에서 전자기록 이용이 보편화됨에 따라 정보화 사회로의 변화가 급속하게 진행되고 있다. 엄청난 양의 정보들이 실시간으로 처리, 보관, 전송되고 있으며 수많은 사용자들에게 편리하고 다양한 정보서비스를 가능케 하였으며 고급정보의 접속 또한 날로 증가하고 있다. 그러나 인터넷상의 각종 서비스가 증가함에 따라 단순히 정보와 자원의 공유에 국한되었던 범위를 넘어 일반인들도 쉽게 전 세계의 정보를 가상 공간상에서 수집이 용이해졌고 또한 이를 악용하는 불건전정보 유통 및 정보범죄와 같은 정보화의 역기능 또한 크게 증가하고 있다[1]. 네트워크상에서의 정보시스템에 대한 침입시도는 해가 갈수록 증가되고 다양화되고 있으며, 침입의 방법도 점차로 자동화 및 지능화 되고 있다. 정보화의 역기능을 초래하고 있는 정보 범죄의 문제에 대하여 시스템의 안정적이면서 효율적인 환경을 제공하기 위해서 네트워크의 병목구간에 위치해서 내부 네트워크를 외부의 불법 사용자로부터 보호하는 역할을 수행하는 침입차단시스템(Firewall)과 컴퓨터 시스템 또는 네트워크의 이벤트의 발생을 감시하고 보안에 관련된 문제에 대한 징후를 탐지하는 침입탐지시스템(Intrusion Detection System)과 같은 정보보안 시스템들이 개발되어 사용되고 있다.

불법적인 시스템 접근을 탐지하기 위하여 사용되고 있는 침입탐지 시스템 중 네트워크상의 보안영역을 설정하고 해당 영역에 전송되어지는 패킷을 수집하여 침입 여부를 판정하는 네트워크 침입탐지 시스템은 실시간으로 전송되어지는

패킷에서 탐지에 필요한 감사자료를 수집하고, 축약하여 침입에 대한 정보를 가지고 있는 침입 패턴과 비교함으로써 불법적인 사용자의 침입을 탐지한다. 그러나 최근 침입탐지 시스템의 탐지 방법과 인터넷망의 표준인 TCP/IP 프로토콜의 구조상 취약점을 이용하여 침입자의 공격사실을 탐지하지 못하도록 하는 IDS 우회공격이 등장하고 있다.

IDS 우회공격이란 침입자가 특정한 공격방법 또는 도구를 사용하여 침입 탐지 시스템이 관리하는 보안영역에 침입을 시도할 때 침입탐지 시스템이 해당 공격에 대해서 침입탐지 서비스를 제공하지 못하는 일련의 취약점을 이용한 공격이다[2]. 이러한 우회공격은 침입탐지 시스템의 목표인 침입자에 의한 불법적인 사용을 탐지하는 것을 어렵게 만들고 침입탐지 시스템에 대한 신뢰도를 저하시키고 있다. 그러나 기존의 네트워크 기반 침입탐지시스템들은 우회공격에 대해 능동적으로 대처하는데 어려움이 많다. 따라서 이를 고려한 새로운 형태의 네트워크 침입탐지 시스템을 제시하여 효율적이고 능동적인 새로운 개념의 침입탐지시스템을 연구 개발할 필요성이 있다.

본 논문에서는 네트워크 패킷을 이용한 우회 공격을 탐지할 수 있는 IDS 우회공격 탐지 시스템을 설계, 구현한다. IDS 우회공격 탐지 시스템 설계를 위해 2장에서 침입탐지 시스템 우회공격 기법을 정의, 분류하고 3장에서는 IDS 우회공격 탐지 시스템 모델을 제안하고 모듈별로 분석하여 설계 및 구현한다. 마지막으로 4장에서 결론 및 향후연구로 끝을 맺는다.

2. 침입탐지 시스템 우회 공격

2.1 침입탐지 시스템

침입탐지 시스템(IDS : Intrusion Detection

System)은 허가되지 않은 사용자로부터 접속, 정보의 조작, 오용, 그리고 남용 등 컴퓨터 시스템 또는 네트워크 상에서 시도됐거나 진행중인 불법적인 예방에 실패한 경우 취할 수 있는 방법으로서 의심스러운 행위를 감시하여 가능한 침입자를 조기에 발견하고 실시간 처리를 목적으로 하는 시스템이다[3][4]. 침입탐지시스템의 기본적인 개념은 James P. Anderson에 의해 1980년대 초에 제시되었으며 Dorothy Denning과 Peter Neumann에 의해 1984년에서 1986년 까지 연구, 개발된 IDES(Intrusion Detection Expert System)에서 처음으로 구체화 되었다 [5].

침입탐지 시스템의 전반적인 구조는 정보수집단계, 정보가공 및 축약단계, 분석 및 침입탐지, 그리고 보고 및 조치단계로 구성되어 있다 [6]. 정보수집단계에서는 호스트나 네트워크 패킷과 같은 정보를 이용하여 데이터를 수집하며, 수집된 데이터는 특정 침입 탐지 모델을 적용하여 분석된다. 분석 결과는 보고 및 조치단계를 통하여 대응 및 후속조치를 수행하게 된다. (그림 1)은 침입탐지 시스템의 기본 구성 요소들을 보여 주고 있다.

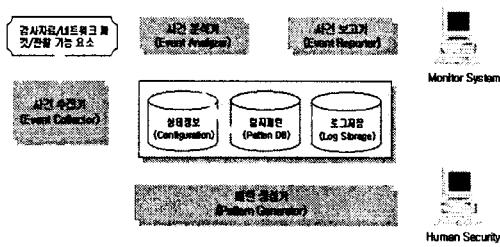


그림 1 침입탐지 시스템의 기본적인 구성

감사자료/네트워크 패킷/관찰가능 요소 대상의 발생은 사건 수집기에 의해서 수집되어 사건 분석기에서 침입여부에 대한 분석을 수행하게 된다. 이러한 과정에서 탐지규칙에 대한

패턴 데이터베이스와 로그가 이용되며, 침입이 발생한 경우 이는 사건 보고기에 의한 정보전달을 통하여 시스템 관리자에게 침입사식을 알리게 된다. 또한 침입탐지 시스템의 신뢰성을 높이기 위해서는 일반적인 서비스와 침입에 대한 패턴을 주기적으로 생성할 필요성이 있으며, 보안 관리자는 패턴발생기(Pattern Generator)를 통해서 새로운 공격방식에 대한 탐지규칙의 생성 및 관리역활을 수행한다.

2.2 우회공격의 정의

침입탐지 시스템은 침입의 대상이 되는 시스템 또는 네트워크 환경 하에서 불법적인 사용자의 행위의 탐지를 목적으로 한다. 우회공격(Evasion)은 침입자가 특정한 공격방법을 사용하여 침입대상 시스템에 대한 침입을 시도할 때 침입탐지 시스템이 정상적인 탐지 서비스를 제공하지 못하는 일련의 약점들을 의미한다[2][7]. 예를 들면 (그림 2)와 같이 공격자(Attack system)에서 공격대상(Victim system)으로 "ATACK"이라는 방법으로 공격을 했을 때 IDS 시스템이 "ATACK"이라는 공격에 대해서 탐지하지 못하였다면 공격자는 "ATACK"이라는 우회공격을 사용하여 공격대상을 공격한 것이다. 이 우회공격 방법은 네트워크 침입탐지 시스템의 취약점을 이용하여 실제 침입임에도 불구하고 침입을 탐지하지 못하게 하는 부정오류(false negative)를 유발시킨다.

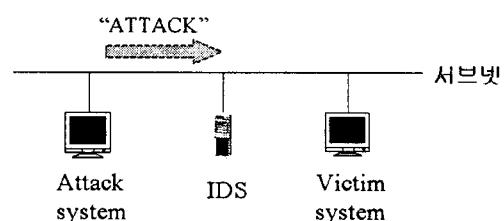


그림 2 침입탐지 시스템 우회공격

네트워크 침입탐지 시스템은 빠르게 전송되는 네트워크 패킷을 분석하여 실시간으로 침입을 탐지하기 위해서 패킷에서 수집된 감사자료와 침입유형 또는 특성이 정의되어 있는 탐지 패턴과 비교하여 침입을 탐지하는 오용탐지 방법을 많이 사용하고 있다. 네트워크 침입탐지 시스템에서 침입을 탐지하는 방법을 간략하게 살펴보면 (그림 3)과 같다.

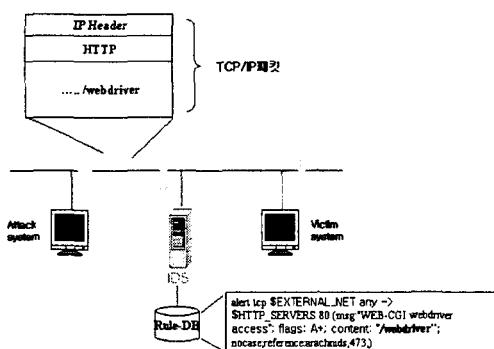


그림 3 침입탐지 시스템과 탐지규칙

소스가 공개되어 있는 일반적인 침입탐지 시스템인 Snort의 규칙 데이터베이스의 규칙 패턴은 다음과 같은 형식으로 되어 있다.

```
► alert tcp $EXTERNAL_NET any ->
$HTTP_SERVERS 80 (msg : "WEB-CGI webdriver access" ; flags : A+ ; content: "/webdriver" ; nocase; reference: arachnids, 473;)
```

네트워크 기반 침입탐지의 보안 구역안에 존재하는 시스템에 공격자가 CGI 버그를 가진 특정한 파일인 webdriver라는 파일을 요청하는 명령을 공격대상(victim)시스템에 전송하면, IDS는 해당공격의 패킷을 캡쳐링하여 시스템 규칙 데이터베이스(Rule-DB)에 정의 되어 있는

탐지 패턴 중 외부의 임의의 IP, 임의의 포트에서 웹서비스를 제공하는 80번 포트로 가는 패킷 중 패킷안에 “webdriver”라는 내용이 있으면 침입으로 판단하여 경고를 보낸다는 것이다. 탐지 패턴을 이용한 네트워크 기반 침입탐지 시스템은 이러한 알고리즘으로 침입을 판단하기 때문에 정의되지 않은 침입에 대해서는 탐지할 수 없게 된다. 공격자들은 이런 취약점을 이용하여 침입탐지 시스템을 우회공격 할 수 있다.

2.3 우회공격 기법 분류

본 논문에서는 네트워크 기반 침입탐지 시스템의 우회공격 방법을 크게 두 가지로 나눈다. 네트워크 패킷의 임의적인 조작 없이 IDS의 탐지패턴을 위조하여 우회 공격하는 방법인 ‘침입 패턴 위조 우회공격’과 패킷을 분할하여 IDS를 우회하는 ‘패킷 분할 우회공격’으로 분류한다.

(1) 패턴위조 우회공격

침입패턴을 위조하는 우회공격 방법은 침입하고자 하는 시스템의 취약점이 존재하는 서비스 또는 파일의 존재여부를 수집하는 “정보수집 단계”에서 많이 사용되어진다. 특히 웹 서비스 상에 존재하는 특정한 취약점 파일을 탐지하기 위한 웹 취약점 탐지 및 RPC버그, 버퍼 오버플로우, 특정 포트를 기준으로 시스템에 접속하는 Trojan프로그램 등의 탐지 규칙을 우회하기 위해 사용된다. 이들 우회 방법은 패턴매칭 우회, URL 기호화, 매개변수 감추기, 긴 URL 등으로 세분할 수 있다.

각 경우의 예를 웹 서비스를 예를 들어 설명 한다. 사용자가 웹서버에 웹서비스를 요청하는 방식은 RFC1945에 정의 되어있는 HTTP 요청의 구성요소를 따르고 있다. 일반적인 웹서비스의 제공은 (그림 4)와 같이 제공되어 진다. 먼저 인터넷 사용자(클라이언트 시스템)에서 웹 서비스 제공자에게 특정한 페이지를 요청하는 URL

주소의 요청은 웹 클라이언트 프로그램은 TCP/IP 프로토콜을 이용하여 웹서비스를 제공하는 서버의 해당포트에 URL에 입력된 특정한 페이지를 요청하는 HTTP 명령어를 전달하게 된다. 사용자가 요청한 명령을 웹서버상에서 수행하고 그 결과를 인터넷 사용자에게 전송해 준다. 일반적으로 웹클라이언트는 웹서버에게 특정한 페이지(HTML 3.2 규약을 이용한 페이지)를 요청하고 웹서버는 요청받은 파일을 웹클라이언트에게 전송해 준다. 전달받은 결과값을 웹클라이언트 프로그램(Netscape, Explorer 등)이 사용자가 볼 수 있는 화면으로 재구성 후 사용자에게 보여 준다.

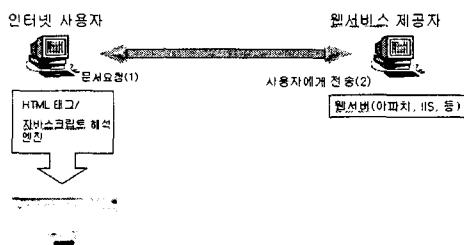


그림 4 웹서비스 개요

RFC1945에 정의 되어있는 HTTP 요청의 구성요소 형식은 다음과 같다.

[GET¹⁾ /cgi-bin/some.cgi²⁾ HTTP/1.0³⁾]

여기에서 1)은 요청 방법에 대한 규정으로 일반적으로 GET, HEAD, POST 등으로 서버에게 데이터 형식을 요청한다. 2)는 요청 페이지 경로로서 상대경로(/cgi-bin/file) 또는 웹서버의 URL을 포함한 절대경로 (http : // server/some/ file)로 표현될 수 있다. 3)은 일반적인 버전 표시로 일반적인 웹서버의 형식 버전 요청 방법, 요청 페이지, 일반적인 버전은 모두 빈칸으로 구분되어 진다.

① 패턴매칭 우회: 사용자가 특정한 파일의

존재 여부를 웹 클라이언트 프로그램을 이용하지 않고 TCP/IP 연결을 확립할 수 있는 텔넷 같은 프로그램을 이용하여 HTTP 요청을 수행한다. 이 경우 일반적인 페이지 요청 형식인 [GET/cgi-bin/some.cgi HTTP/1.0] 대신 GET과 같은 역할을 하는 [HEAD /cgi-bin/some.cgi HTTP/1.0]으로 변경하여 해당 CGI 파일을 요청한다. 만일 침입탐지 시스템에 HEAD라는 명령어에 대한 탐지 규칙이 정의되어 있지 않다면 이 요청을 탐지할 수 없다.

② URL 기호화(URL encoding): 전형적인 방법으로 HTTP 프로토콜 규약에는 URL에 사용할 수 없는 프린트 불가능 문자, 특수 문자, non-ASCII 문자들을 URL에 사용하고자 할 때 문자들을 기호화하여 사용할 수 있다. 이러한 인코딩 방법에는 UFT와 Hex 엔코딩 방법이 많이 사용된다. 공격자는 '='라는 단어 대신에 '%2B'를 '='는 '%3d'로 공백은 '%20'으로 NULL값은 '%00'으로 변환하여 URL에 요청한다. 이러한 URL 기호를 이용하여 사용자 특정 페이지에 대한 요청을 하는 경우 탐지 규칙이 엔코딩되지 않은 스트링으로 정의된 탐지 패턴을 우회할 수 있다.

③ 매개변수 은닉: 인터넷 서비스 제공자는 매개변수(parameter)를 이용하여 사용자로부터 특정한 값을 전달받을 수 있는 방법을 제공한다. 이러한 방법은 인터넷 서비스 제공자에 존재하는 파일이 사용자로부터 특정한 값을 입력받아 수행하는데 필요하다. 형식은 URL 뒤에 매개변수를 입력받아 수행되어져야 하는 파일 뒤에 '?'을 삽입하고 매개변수 값을 입력해 주면 된다. 일반적인 침입탐지 시스템은 URL 부분에 '?'표(또는 %3F)가 나오면 사용자의 입력 값은 변경이 심하여 특정한 규칙을 적용할 수 없기 때문에 시스템

의 효율성을 위하여 값의 크기만을 검사한다. 만약 '?' 뒤에 변수 값이 아닌 특정한 페이지를 정해주면 인터넷 서비스 제공 프로그램은 매개변수를 값으로 인식하지 않고 페이지의 요청으로 인식한다. 이러한 점을 이용하여 URL 뒤에 매개변수를 입력받아 수행되어져야 하는 파일 뒤에 %3Fpappm을 입력하고 특정 페이지를 요청할 수 있다.

- ④ 긴 URL: 침입탐지 시스템의 침입탐지 알고리즘에서 침입탐지 시스템의 성능을 향상시키기 위해 HTTP 프로토콜을 이용한 웹서비스 요청 패킷에 대해서는 첫 번째 라인에 요청한 페이지에 대한 정보가 들어 있기 때문에 패킷의 빠른 처리와 탐지를 위해서 패킷의 데이터 부분에 일정한 크기의 바이트만을 검사하는 방법을 많이 사용한다. (그림 5)와 같이 아무런 역할을 하지 않는 캐릭터 부분을 충분히 삽입하여 요청 페이지가 침입탐지시스템이 검사하는 범위를 벗어나게 하는 방법이다.

IP
HTTP
GET <lots of characters> rfp /./cgi-bin/some.cgi HTTP/1.0

← 탐지부분

그림 5 Long URL 회피공격

(2) 패킷분할 우회공격

패킷분할 우회공격방법은 서로 다른 최대 패킷 사이즈의 제한을 가진 이 기종의 네트워크 환경에서 IP 패킷의 효율적인 전송을 보장해 주고 있는 IP 단편화(fragmentation) 방법에 대한 취약점을 이용하는 방법이다. 즉 정상적인 크기의 패킷을 임의의 개수의 패킷으로 분할하여 보안영역에 존재하는 시스템에 침입을 시도하는 방법이다. IP

단편화는 IP 데이터 그램이 네트워크를 통해 전송될 때, 전송되는 IP 데이터 그램의 크기가 해당 전송 매체에서 전송될 수 있는 최대 크기 즉, MTU(Maximum Transmission Unit)보다 클 경우 발생한다[11]. (그림 6)과 같이 이더넷에서 전송 가능한 IP 데이터 그램의 최대 크기 즉 MTU는 1500바이트이고 전송하고자 하는 사용자의 데이터가 1500 바이트보다 큰 경우 IP 분할이 필요하다. 이때 각 패킷 각각의 조각을 프ラ그먼트(fragment)라 하며 시스템 및 네트워크 장비에서 이러한 패킷을 프래그먼트화 하는 작업을 단편화(fragmentation)라 한다. (그림 7)은 단편화된 프라그먼트 패킷의 IP 헤더의 내용을 간략히 설명하고 있다.

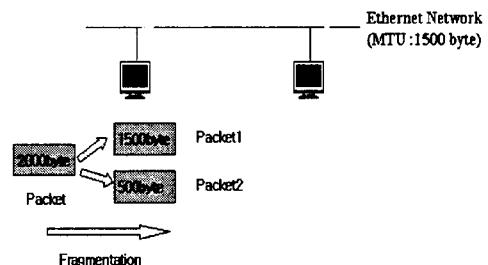


그림 6 IP Fragmentation

네트워크기반 침입탐지 시스템이 분할된 패킷에 대해서 침입을 탐지하기 위해서는 목적지 시스템에 전송되어 단편화되기 전의 상태로 복구되어야 만이 전송하고자 했던 원래의 데이터를 인식할 수 있게 된다. 그러나 기존의 네트워크 기반 침입탐지 시스템의 성능향상을 위해서 패킷을 캡처하여 분할된 첫 번째 패킷만을 검사하므로 이러한 공격은 대부분의 침입탐지 시스템을 우회할 수 있다.

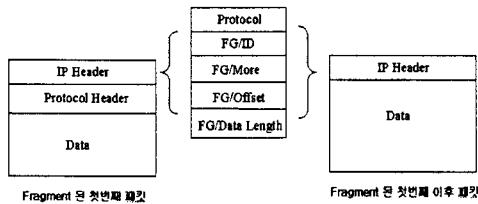


그림 7 Fragment 패킷의 형태

<표 1> 단편화된 패킷 정보

Protocol	TCP, UDP, ICMP등과 같은 프로토콜에 대한 정보를 가지고 있다.
FG/ID	패킷을 재조립하기 위한 식별 번호, IP 헤더의 16비트 필드로써 "IP identification number" 또는 "fragment ID"로 불린다.
FG/More	추가적인 fragment들이 있을 경우 ME (More Fragment) flag를 1로 설정된다.
FG/offset	각 fragment는 원래 fragment 되기 이전의 패킷에서의 위치 즉 "fragment offset" 을 가진다.
FG/Data length	각 fragment는 그 fragment의 데이터 길이를 가진다.

① 작은 단편화(tiny fragmentation) 공격: 네트워크 침입탐지 시스템 및 패킷필터링 장비는 패킷의 필터링을 결정하기 위해 포트를 확인한다. 만약 패킷에 포트 번호가 포함되지 않을 정도로 아주 작게(tiny) 단편화된 첫 번째 패킷을 전송하면 필터링 규칙에 적용되지 않기 때문에 침입탐지 시스템을 우회할 수 있다. 또한 실제적인 포트 번호는 첫 번째 이후의 패킷에 포함하여 전송된다. 그러나 단편화된 패킷

에 대하여 첫 번째 패킷만을 검사하는 기준의 침입탐지 시스템은 이러한 패킷을 검사하지 않고 통과시키게 된다. 이러한 점을 이용하여 공격자는 침입탐지 시스템이 보호해야 할 목적지 서버에 공격 패킷을 작은 단편화 공격을 수행하면 침입하고자 하는 시스템에서 패킷들이 재조합되므로 공격자가 원하는 포트의 프로그램을 수행 할 수 있다.

② 패킷중첩(overlap) 공격: 작은 단편화와 유사한 방법을 사용하는 공격으로 작은 단편화가 단순히 패킷을 분할하여 포트 번호를 감추는 방법이라면, 패킷중첩은 패킷이 재조립될 때 이용되는 프ラ그먼트 오프셋(offset) 번지를 위조하여 두 번째 패킷의 값이 첫 번째 패킷의 값에 덮어쓰도록 하여 포트번호를 위조하는 것이다. 이러한 공격은 침입탐지 시스템이 첫 번째 패킷의 포트번호가 존재하지 않을 때에는 패킷을 폐기한다는 규칙을 가진 IDS를 우회할 때 사용되어진다. 첫 번째 프라그먼트 패킷에서는 패킷 필터링 장비에서 허용하는 http(TCP80) 포트와 같은 포트 번호를 가지고 전송하고, 두 번째 프라그먼트 패킷에서는 오프셋 번지를 조작하여 패킷들이 재조합될 때 두 번째 프라그먼트 패킷이 첫 번째 프라그먼트 패킷의 일부분을 덮어쓰도록 새로운 형태의 패킷이 재조립된다. 따라서 공격자는 원하는 포트 번호의 값을 가진 패킷을 전송하게 된다. IDS에서는 첫 번째 프라그먼트 패킷은 허용된 포트 번호이므로 통과시키고, 두 번째 프라그먼트 패킷은 이전에 이미 허용된 프라그먼트 패킷의 ID를 가진 패킷이므로 역시 통과시키게 된다. 이 두개의 프라그먼트 패킷이 목적지 서버에 도착하여 재조립되면 첫 번째 프라그먼트의 포트

번호는 두 번째 프로그먼트의 포트번호로 중첩(overwrite)되고 TCP/IP 스택은 이 패킷을 응용프로그램에 전달한다.

- ③ 비정상적 오프셋 값을 갖는 패킷분할: 첫 번째 프로그먼트 패킷은 정상적이고, 두 번째 프로그먼트 패킷은 첫 번째 패킷의 데이터의 길이보다 더 작은 오프셋 값을 가지고 전송되어 침입하고자하는 시스템에서 분할된 패킷을 재구성한 후의 최종 패킷은 실제적으로 완전히 다른 정보를 가지고 수행되게 된다. (그림 8)은 중첩된 패킷을 도식화 한 것이다.

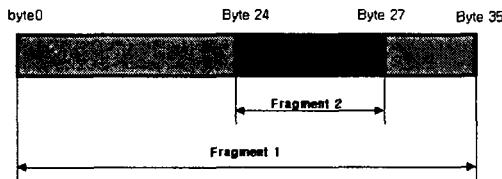


그림 8 중첩된 패킷

- ④ 음의 오프셋 값: 일부 구버전의 운영체제는 단편화된 패킷을 재구성하려 할 때 두 번째 단편화된 패킷의 오프셋 값을 음의 값으로 처리하도록 유도할 수 있다. 이러한 오프셋 값을 통해 메모리 복사(copy) 작업을 수행하게 된다. 메모리 복사는 음의 값을 가지고 수행될 수 없기 때문에 작은 음의 값을 처리하게 유도하여 많은 양의 메모리 복사작업을 수행하게 한다. 이러한 방식으로 시스템의 기능장애를 유발시킨다.

3. 우회공격 탐지 시스템

IDS 우회공격 탐지 시스템은 기존의 침입탐

지 시스템의 탐지패턴의 변경 없이 우회공격이 의심되는 패킷을 재조립하여 탐지패턴에 적용시킨다. 이는 우회공격기술이 독립적인 하나의 공격 패턴이 아닌 기존의 침입기술을 네트워크기반 침입탐지 시스템에서 탐지되지 못하도록 하는 방법을 사용하기 때문이다.

3.1 구현환경

우회공격 탐지 시스템은 Linux를 기반으로 구현하였다. 시스템 구현을 위해 C/C++을 사용하였으며, 패킷 수집을 위한 패킷 필터로는 Libpcap 4.0을 이용하여 구현하였다. 본 시스템은 네트워크 상에 보안영역을 설정하여 해당 영역으로 전송되어지는 패킷만을 조사하여 침입을 탐지한다. 보안 영역은 이더넷 프레임에서 수집할 수 있는 목적지 주소를 특정한 호스트나 서브넷으로 한정하여 설정하였다.

3.2 시스템 구성 및 구현

우회공격 탐지 시스템의 구성은 (그림 9)와 같이 감사자료 수집 모듈과 침입탐지 모듈 및 보고 모듈로 구성되어 있다. 네트워크 인터페이스 카드는 PROMISCOUS 모드로 설정하여 자신의 네트워크를 지나가는 모든 패킷을 캡처링하여 패킷의 목적지 주소가 설정되어진 보안구역에 해당하는 패킷만에 대해 침입을 탐지한다. IDS 우회공격 탐지 시스템의 구성은 기존의 침입탐지 시스템의 탐지 규칙을 변경하지 않고 규칙을 추가하여 우회공격을 탐지한다는 설계 목적을 기반으로 한다. 따라서 기존의 네트워크 기반 침입탐지 시스템의 패킷수집 모듈과 침입보고 모듈은 그대로 사용하였으며[8], 감사자료 수집 모듈과 침입탐지 모듈은 EDS(Evasion Detection System)모듈의 목적에 맞게 재구성하였다.

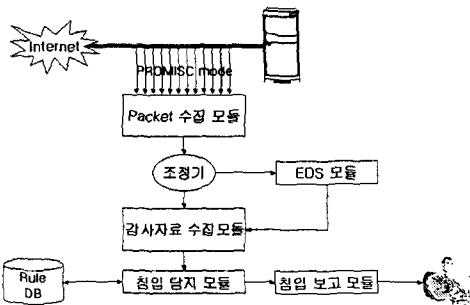


그림 9 IDS 우회공격 탐지시스템 모델

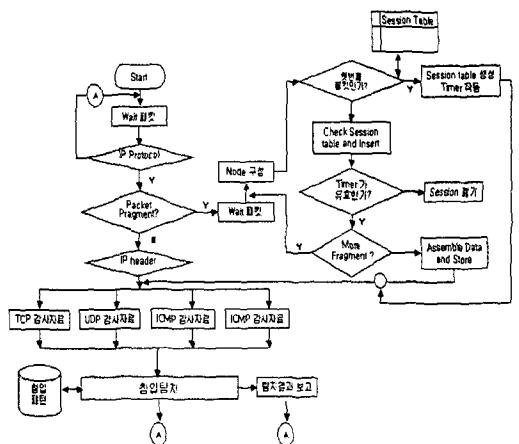


그림 10 우회공격 탐지 알고리즘

패킷 수집 모듈의 감사자료 수집은 시스템의 효율을 위해서 두 가지의 형태로 구성되어 있다. 수집되어진 패킷이 우회공격의 의심이 없는 정상적인 IP 패킷이면 프로토콜의 데이터 타입에 따라 기본적인 발신자 주소와 수신자 주소 그리고 서비스에 따른 포트 번호 및 사용자의 모든 데이터를 추출하고, 우회공격이 의심되는 분할된 패킷이면 네트워크 침입탐지 시스템의 탐지 규칙에 적용할 수 있는 데이터로 구성하기 위해 패킷을 재조립하는 EDS 모듈에 전송한 뒤 완전한 패킷의 형태로 구성하여 TCP/IP 프로토콜 데이터 타입에 따라 감사자료를 추출한다. 침입탐지 모듈은 탐지규칙을 분석하여 기존의 침입탐지 규칙에 새로이 우회 공격을 탐지하는 규칙을 추가하여 개선된 규칙 데이터베이스(rule DB)를 작성하였으며, 보고 모듈은 침입탐지 모듈에서 탐지한 결과를 관리자에게 시스템의 콘솔 및 이메일로 보고하는 기존의 모듈을 그대로 사용하였다.

(1) 패킷수집 모듈

패킷 수집은 버클리 대학에서 개발하여 모든 유닉스 시스템에서 사용 가능한 libpcap 라이브러리를 이용하였으며 네트워크 인터페이스를 Promiscuous 상태로 변경하여, 네트워크상에서 패킷을 수집한다. libpcap 라이브러리를 이용하여 패킷을 추출하는 과정은 (그림 11)과 같다.

현재 시스템에 설치되어 있는 NIC (Network Interface Card)의 상태, 버퍼의 크기 및 넷마스크를 체크하여 아무런 이상이 없다면 패킷을 수신한다. 수신되어진 패킷은 프로그램 실행 시 주어지는 패킷 필터링 규칙에 의해 사용자가 원하는 패킷만 얻을 수 있다. 본 논문에서는 인터넷 프로토콜인 TCP/IP 프로토콜 중 IP, TCP, UDP, ICMP 관련 패킷만을 필터링 한다.

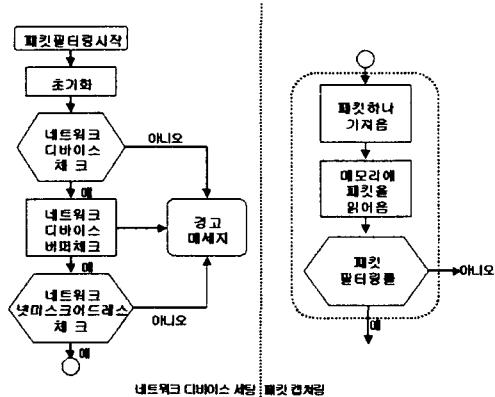


그림 11 libpcap을 이용한 패킷 추출

(2) 우회공격 탐지 모듈

인터넷을 사용하여 데이터의 정보전달은 패킷이라는 단위를 이용하여 전달되어 진다. 만일 하나의 패킷이 너무 커서 하나의 단위로 전송되어 질 수 없을 때, 네트워크를 통해 보내어질 수 있는 두 개 이상의 더 작은 패킷조각으로 분리되어 쳐야 한다. 프로그먼트 패킷을 이용하는 우회공격 탐지를 하기 위해서는 단편화된 패킷을 완전한 형태로 구성해서 감사자료를 수집할 수 있도록 감사자료 수집모듈에 전송해 주어야 한다. 패킷의 재구성은 연결 리스트(linked list)를 이용하여 확장성을 보장하고 패킷의 재조립을 쉽게 유도하였다. 먼저 수집되어진 패킷의 형태가 IP 프로토콜을 가지고 있으면 IP헤더의 정보 중 FG/ID 즉, 패킷을 재조립하기 위한 식별 번호가 존재여부를 검사하여 단편화된 패킷인지를 판단한다. 만약 단편화된 패킷이면 오프셋 번지를 검사하여 첫 번째 단편화 패킷인지 아닌지를 판단하여 2가지의 형식 중 해당되는 노드에 저장한다. 같은 방법으로 이어져 도착하는 프로그먼트 패킷에 대해서도 노드를 구성하여 같은 식별번호를 기준으로 마지막 프로그먼트 패킷이 도착할 때까지 연결 리스트를 구성하게 된다.

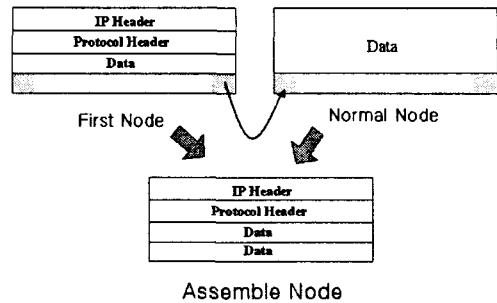


그림 12 패킷 재조립

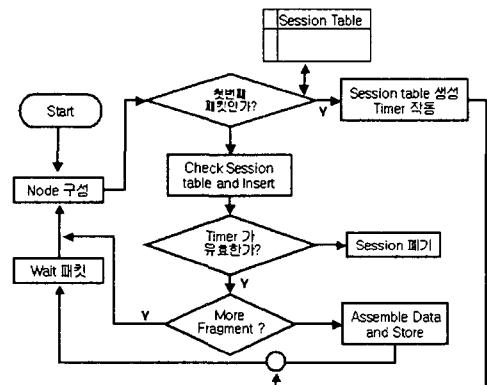


그림 13 패킷 재조립 과정

마지막 노드가 완성이 되면 (그림 12)와 같이 패킷 재조합을 거치게 된다. 재조립되어진 패킷의 정보를 감사자료 수집 모듈로 전달한다.

(3) 감사자료 생성 모듈

패킷 수집 프로그램을 이용하여 네트워크에 흘러 다니는 패킷을 수집할 수 있으나 수집된 패킷은 여러 가지 많은 정보를 포함하고 있다. 많은 정보들 중 침입탐지 시스템의 탐지 패턴에 적용되어지는 정보만을 추출하는 모듈이 감사자료 생성 모듈이다. 패킷 필터링 모듈에

서 이더넷 프레임 전체로 받기 때문에 일단 이더넷 계층에서 IP인지 ARP 패킷인지를 나눠야 하며 또한 IP 계층에서 ICMP인지 TCP 인지 UDP인지를 나눠야 한다. 본 논문에서는 IP 계층에서 TCP와 UDP 그리고 ICMP로 나누어 각각의 프로토콜의 특성에 맞게 감사자료를 생성한다.

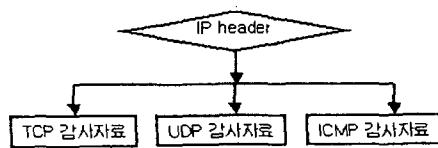


그림 14 패킷 타입별 감사자료 수집

(4) 침입탐지 모듈우회공격 탐지 모듈

침입탐지 모듈은 감사자료 수집 모듈에서 생성된 정형화된 데이터를 이용하여 침입을 탐지한다. 침입 탐지 모듈은 감사자료 수집 모듈에서 TCP와 UDP등을 서로 다른 큐에 저장한 패킷을 하나씩 꺼내어 탐지한다. 이때 각각의 큐에서 하나씩 꺼내어 탐지할 때는 감사 수집 모듈에서는 세마포어를 증가시키며 큐에서 빠져나갈 때는 세마포어를 감소시켜서 큐에 대한 동기화를 시킨다. 탐지 모듈은 TCP, UDP, ICMP 등의 각각의 큐에 하나씩 쓰레드가 있기 때문에 동기화를 시켜주게 된다. 침입탐지 방법은 네트워크 패킷의 기본적인 감사자료를 바탕으로 침입을 탐지하는 '단일감사자료 비교'를 통한 탐지방법'과 단일감사자료를 시간에 대해서 비교 분석하여 탐지하는 '시간에 대해 축적된 감사자료를 통한 탐지 그리고 네트워크 패킷상에 존재하는 사용자의 명령어를 통하여 침입을 탐지하는 '임의 사용자의 명령어 및 아규먼트의 분석 결과를 침입패턴과 비교하여 탐지'로 나눌 수 있다.

- ① 단일 감사자료 비교를 통한 탐지: 프로토

콜에 따름 감사자료의 서비스유형, 목적지 주소, 발신지주소, 서비스요청포트 등을 그대로 침입탐지 패턴 규칙과 비교하는 방법을 사용한다. 이러한 탐지 규칙으로는 land attack, ping flooding, Trojan, smurf attack 등을 탐지한다.

- ② 시간에 대해 축적된 감사자료를 통한 탐지: 단일 감사자료 비교를 통한 탐지에 시간을 부여하여 일정한 시간 간격동안 수집되는 감사자료를 침입탐지 패턴과 비교하는 방법을 사용한다. 이러한 탐지 규칙으로는 취약점 스캐너 공격(mscan,sscan,nmap 등)을 탐지 한다.
- ③ 임의 사용자의 명령어 및 아규먼트의 분석결과를 침입패턴으로 비교하여 탐지: 수집되는 감사자료중 사용자의 명령어와 아규먼트 중 침입에 사용되어지는 악의적인 명령어와 아규먼트가 정의되어 있는지를 탐지 규칙과 비교하여 침입을 탐지한다. 이러한 탐지 규칙으로는 웹서버 취약점 공격(cgi버그, php버그, IIS의 unicode 버그...) 및 시스템취약점 공격(Buffer Overflow) 등을 탐지한다.

(5) 침입보고 및 대응 모듈

네트워크에서 수집된 감사자료를 이용하여 침입판정모듈에서 침입이 탐지되면 관리자에게 침입의 결과를 보고하게된다. 침입보고는 시스템의 콘솔, 전자우편 등을 이용하여 침입의 사실을 보고하게 된다. 네트워크에서 수집된 감사자료를 이용하여 침입판정모듈에서 침입이 탐지되면 관리자에게 침입의 결과를 보고하게 된다. 시스템 콘솔은 침입의 사실을 보여주게 되며, 전자우편 보고는 arin.net, whois.apnic.net, whois.krnic.net 등에서 whois 서비스를 이용하여 침입자의 정보를 파악한 후 첨부하여 관리자에게 보내진다.

제4장 결론 및 향후 연구과제

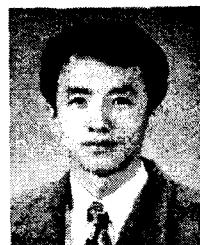
침입탐지시스템에서 우회공격 탐지의 중요한 이유는 우회공격이 새로운 특정한 공격 방법을 사용하는 것이 아닌 기존에 존재하는 공격 방법이 탐지되지 않도록 우회하는 기술을 제공하기 때문이다. 이러한 우회공격은 점차 지능화, 분산화, 자동화 되어가는 기존의 침입과 함께 사용되기 때문에 정확한 탐지를 어렵게 만들며, 침입탐지 시스템에 대한 신뢰도를 저하시키고 있다. 기존의 네트워크 기반 침입탐지시스템들은 우회공격에 대해 능동적으로 대처하는데 어려움이 많다. 따라서 우회공격에 대비한 효율적이고 능동적인 새로운 형태의 침입탐지시스템을 연구 개발할 필요하였다. 본 논문에서는 네트워크 침입탐지 시스템의 취약점을 이용하여 침입탐지시스템에 탐지되지 않는 침입탐지시스템 우회공격에 대해 분석하고 탐지 방법을 제안하였다. 또한 제안된 알고리즘을 적용한 침입탐지시스템 우회공격 탐지 시스템을 개발, 운영하여 방법의 타당성을 입증하였다.

네트워크 패킷은 연속적으로 발생되기 때문에 탐지 알고리즘의 처리가 늦어지게 되면 연속해서 들어오는 패킷의 손실이 발생하게 된다. 따라서 거짓탐지율과 탐지실패율을 최소화하는 범위 내에서 탐지 알고리즘을 단순화할 필요가 있다. 또한 새로운 우회공격 유형에 대한 탐지 방법은 계속 연구되어야 할 과제이다.

참고문헌

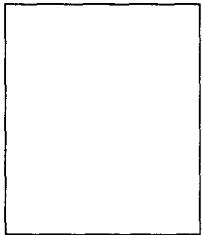
- [1] 최용락 외 3인, 통신망 정보 보호, 도서출판 그린, 1997.
- [2] Steve Schupp Limitation of Network Intrusion Detection, <http://www.sans.org>, December, 2000.

- [3] D.E. Denning, "An Intrusion-Detection Model", IEEE Trans on Software Engineering, No. 2, Feb., 1998.
- [4] M. Esmaili, R. Safavi-Naini, and J. Pieprzyk, "Intrusion Detection: a Survey", ICCC95, PP409-414, 1995.
- [5] T.F. Lunt, "A Survey of Intrusion Detection Techniques", Computer & Security, Vol. 12, No. 4, Jun., 1993.
- [6] R. G. Bace, Intrusion Detection, Macmillan Technical Pub, 2000.
- [7] Fred Cohen, 50 ways to Defeat Your Intrusion Detection System, <http://all.net/>, 2001.
- [8] Brad Sanford, IP Fragmentation and Fragrouter, http://www.sans.org/infosecFAQ/encryption/IP_frag.html, 2001.
- [9] 이극 외, 네트워크 침입탐지 기술 연구, 한국 전자통신연구원 보고서, 1999.
- [10] Vern Paxson, Bro:A System for Detecting Network Intruders in Real-time, Lawrence Berkeley National Laboratory, January, 1998.
- [11] Steven McCanne, Van Jacobson, The BSD Packet Filter: A New Architecture for User-level Packet Capture, December, 1992.
- [12] 박정호 외, 호스트기반 침입탐지 시스템 개발에 관한 연구, 한국정보보호센터 보고서, 1998.



길민옥

1989년 한남대학교 전자계
산공학과 공학사
1991년 한남대학교 전자계
산공학과 공학석사
2000년 한남대학교 전자계
산공학과 공학박사
1997년 ~ 현재 문경대학 인터넷정보계열 조교수
관심분야 : 정보보호, 보안시스템, 인공지능, 음성인식, 멀티미디어, 유전자 알고리즘



차 준 남

2000년 한남대학교 컴퓨터
공학과 공학사
2002년 한남대학교 컴퓨터
공학과 공학석사
관심분야: 정보보호, 보안시
스템, 인증



이 극

1983 경북대학교 전자공학
과(전산모듈) 공학사
1986년 서울대학교 컴퓨터
공학과 공학석사
1993년 서울대학교 컴퓨터
공학과 공학박사

1988년 ~ 현재 한남대학교 정보통신멀티미디어
학부 컴퓨터공학전공 교수
2001년 ~ 현재 한남대학교 부설 정보보호응용기
술연구소 소장
관심분야 : 정보보호, 보안시스템, 인공지능, 멀
티미디어, 생체인식