IP 단편화 공격 탐지를 위한 NIDS

김성환, 조성제, 정승익, 김현종, 정태일, 최영복
동명정보대학교 정보통신공학과
e-mail : si12019@hotmail.com

NIDS for IP Fragmentation Attack Detection

Sung-hwan Kim, Sung-je Cho, Seung-ik Jeong, Hyun-jong Kim, Tae-il Jeong, Young-bok Choi
Dept. of Communication Engineering Dongmyung University of Information Technology

요 약

IP 단편화는 서로 다른 네트워크 환경에서 IP 패킷의 효율적인 전송을 보장해 주고 있다. 하지만 시스템이 비정상적인 IP 단편을 적절히 재조합하지 못함으로써 시스템에 심각한 문제를 일으킬 수 있다. 그래서 본 논문에서는 네트워크 상에서 IP 단편화 공격을 탐지할 수 있는 방법을 제안한다. 제안한 방법은 IP 단편화 공격에 대해서 TCP 패킷을 NIDS가 미리 재조합을 함으로써 IP 단편화 공격에 대해 효율적인 탐지가 가능하다.

1. 서론

네트워크와 컴퓨터의 발달로 인해 지금의 시대는 컴퓨터 사용자들이 빠르고 쉽게 인터넷을 통해서 필요한 정보를 얻을 수 있게 되었다. 그러나 이와 같은 네트워크와 컴퓨터의 발달로 인해서 다른 문제점들이 생겨나게 되었다. 그 중에 가장 큰 이유 중 하나가 바로 크래킹 기술 발달로 인해 개인 신상 정보 유출, 상업기관이나 공공기관의 서버 중단과 같은 피해가 속출하고 있기 때문이다. 크래킹 즉, 침입이란 비 인가된 사용자가 자원의 무결성(Integrity), 기밀성(Confidentiality), 가용성(Availability)을 저해하는 일련의 행동들과 보안정책을 위반하는 행위를 말한다[1-3].

현재까지 이러한 크래킹 기법으로 인한 피해를 줄이기 위한 방법으로 침입 차단 시스템(FW:Fire Wall)과 침입 탐지 시스템(IDS:Intrusion Detection System) 등이 개발되어 왔는데 침입 탐지 시스템(IDS)이 침입 차단 시스템(FW)에 이은 차세대 보안 솔루션으로 부각되는 주된 이유는 침입 차단 시스템이 효과적인 차단에 실패하였을 경우, 이에 따른 피해를 최소화하고 네트워크 관리자 부재 시에도 해킹에 적절히 대응할 수 있는 보안 솔루션에 대한 요구가 증가하고 있기 때문이다. 침입탐지 시스템은 침입차단 시스템이 단순한 룰에 따라 불법 침입을 차단하는데 따른 보안상의 한계점을 보완한다[4].

이러한 침입 탐지 시스템에도 단점이 있는데 가장 큰 문제점은 패킷 재조합 기능을 제공하고 있지 않아 공격자가 공격 패킷을 다수의 데이터그램으로 쪼개서 공격할 경우 이를 차단하거나 탐지하지 못하는 경우가 있다는 것이다.

인터넷 프로토콜(IP:Internet Protocol) 단편화(fragmentation)를 이용한 공격에 대한 탐지를 하는데 있어서 보다 효율적으로 방어할 수 있는 방법을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장 관련연구에서는 IP 단편화의 이론적 배경 및 공격 방법을 설명하고, 3장에서는 IP 단편화 공격 탐지 알고리즘을 구현한다. 4장에서는 논문과 관련된 결론을 맺고 향후 연구 방향을 기술한다.

2. IP 단편화와 공격 기술의 종류

2.1 IP 단편화

네트워크로 연결된 각 데이터 링크 계층은 프레임(frame) 형식을 가지고 있다. 프레임 형식에 정의된 필드중의 하나가 바로 필드의 최대 크기

```
[root@mcs /map-2.53]#nmap -f -p 23 -sS 210.110.146.211
Starting nmap V. 2.53 fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on inscure.kisa.or.kr ( 210.110.146.211 ):
Port  State  Service
23/tcp open   telnet
Nmap run completed -- 1 IP address ( 1 host up ) scanned in 0 seconds
```

그림 2. Tiny Fragment 공격 예

이다. 데이터그램(Datagram)이 프레임 속에 캡슐화될 때 데이터그램의 크기는 이 최대 크기보다 작아야 한다.

만약 MTU(Maximum Transfer Unit)가 큰 프로토콜을 사용한다면 패킷의 전달이 효율적이 될 수 있을 것이다. 그러나 다른 네트워크에서는 데이터그램을 나누어서 보내야 한다. 이것을 단편화라고 한다. MTU의 값은 네트워크 프로토콜마다 조금씩 다르다. 그 중 이더넷(Ethernet) 프레임은 MTU의 값은 1500byte이다. 데이터그램이 1500byte보다 크고, Ethernet 네트워크를 통과해야만 한다면 그 데이터그램은 단편화가 필요하게 된다[5-6].

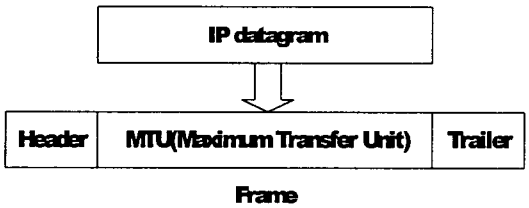

그림 1. MTU

IP 데이터그램의 단편화와 재조립과 관련된 필드는 식별자, 플래그, 단편화 오프셋으로 구성되어있다. 식별자(Identification)는 발신지 호스트로부터 나온 데이터그램을 유일하게 식별한다. 즉, 모든 단편은 같은 식별자 값을 가진다. 플래그(Flag)는 사용하지 않는 비트,do not fragment 비트, more fragment비트로 구성되어 있다. 단편화 오프셋(Fragmentation offset)은 데이터그램 내에서 단편의 상대적 위치를 나타내며, m/8의 값을 가진다.(m=전체 데이터길이-1/단편화 개수)

2.2 단편화를 이용한 공격 기술

2.2.1 Tiny Fragment 공격

Tiny Fragment 공격은 최초의 단편을 아주 작게 만들어서 네트워크 침입 탐지 시스템이나 패킷 필터링 장비를 우회하는 공격이다. TCP(Transmission Control Protocol) 헤더가 2개의 단편에 나누어질 정도로 작게 쪼개서 목적지 TCP 포트번호가 첫 번째 단편에 위치하지 않고 두 번째 단편에 위치하도록 한다[1,4,7].

그림 2는 잘 알려진 스캔 툴인 nmap으로 210.110.146.211 서버로 Tiny Fragment 공격하는 예를 보여준다. TCP 헤더를 몇 개의 단편으로 나누어서 스캔하기 위하여 nmap에 '-f' 옵션을 사용한다.

공격한 서버는 텔넷 서비스가 제공되고 23번 포트가 열려 있는 것을 알 수 있다. 그림 3은 그림 2에서 수행한 공격을 TCP dump를 이용해서 모니터링 한 것이다.

```
00:46:55.522076 210.110.146.226.45229 > 210.110.146.211.telnet: S [bad hdr length] (frag
57513:16@0+)
00:46:55.522298 210.110.146.226 > 210.110.146.211: (frag 57513:4@16)
00:46:55.522339 210.110.146.211.telnet > 210.110.146.226.45229: S 2120789957:2120789957(0)
ack 642488212 win 584 <mss 1460> (DF)
00:46:55.522630 210.110.146.226.45229 > 210.110.146.211.telnet: R 642488212:642488212(0)
win 0 (DF)
```

그림 3. TCP dump를 이용한 모니터링 결과

그림 3에서 볼 수 있듯이 첫 번째 단편 크기는 16바이트로 아무런 옵션이 없을 경우의 TCP 헤더 크기인 20바이트 보다 작은 것을 볼 수 있다. 그리고 나머지 TCP 헤더 4바이트는 두 번째 단편에 있다. 패킷필터링 장비나 침입탐지시스템은 필터링을 결정하기 위해 포트번호를 확인하는데 포트 번호가 포함되지 않을 정도로 아주 작게 단편화된 첫 번째 단편을 통과 시킨다. 또한 실제 포트 번호가 포함되어 있는 두 번째 단편은 아예 검사도 하지 않고 통과 시킨다. 그 결과 보호 되어야 할 목적지 서버에서는 이 패킷들이 재조합되어 공격자가 원하는 포트의 프로그램으로 무사히 연결될 수 있다.

2.2.2 Fragment Overlap 공격

Tiny 단편화 공격기법에 비해 좀더 정교한 공격이다. 첫 번째 단편화에서는 패킷 필터링 장비에서 허용하는 http(TCP 80)포트와 같은 포트번호를 가진다. 그리고 두 번째 단편화에서는 offset을 아주 작게 조작해서 단편들이 재조합될 때 두

번째 단편이 첫 번째 단편의 포트 번호가 있는 부분까지 덮어씌운다. NIDS에서는 첫 번째 단편이 허용된 포트번호이므로 통과시키고 두 번째 단편도 허용된 단편의 ID를 가진 단편이므로 역

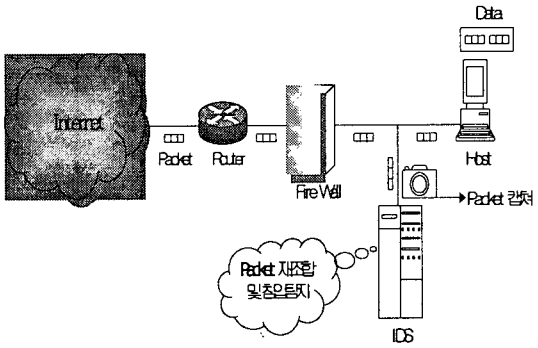

그림 5. 제안한 NIDS 모델

시 통과시킨다. 이 단편들이 목적지에 도달되어서 재조합되면 첫 번째 단편의 포트 번호는 두 번째 포트 번호로 overwrite되고 이 패킷은 필터링 되어야할 포트의 응용프로그램에 전달되어진다.

3. 재조합 기능을 가진 NIDS 모델

3.1 기존의 NIDS 모델

NIDS(Network Intrusion Detection System)은 네트워크 패킷 데이터를 분석하여 침입 탐지에 사용하는 IDS이다. Promiscuous 모드로 동작하여 지나가는 패킷의 헤더와 데이터를 수집, 침입 여부를 판단한다. 대부분 TCP/IP를 사용하는 이더넷(Ethernet)을 주 대상으로 한다. 네트워크 기반의 IDS는 트래픽을 감시할 수 있는 몇몇 위치에만 설치하므로 초기 구축비용이 저렴하고 OS에 독립적이므로 구현 및 관리가 쉽다. 그리고 캡쳐된 트래픽에 대해서는 침입자가 흔적을 제거하기 어렵다.

그림 4에서 기존의 NIDS 모델은 패킷이 들어오면 패킷 매칭 기법을 통해서 네트워크 패킷 데이터를 데이터베이스와 비교, 분석하여 악성 코드로 판명되면 경고 메시지를 발생하는 방식이다. 그러나 재조합 기능이 없기 때문에 IP 단편화를 이용한 공격에는 약한 면이 있다.

3.2 제안한 NIDS 모델

앞서 설명한 기존의 NIDS의 취약성을 보완하기 위해서 새로운 기능 즉, 재조합 기능을 하는

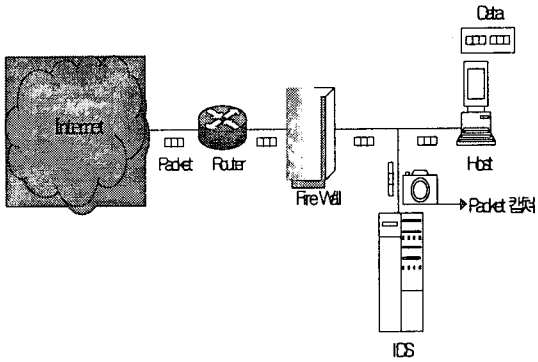

그림 4. 기존의 NIDS 모델

모듈을 IDS 엔진에 추가한다면 IP 단편화를 이용한 공격을 탐지할 수 있다.

공유 메모리에 패킷을 복사하여 fragment ID, fragment offset과 more fragment를 보고 순서대로 조합하여 그 패킷이 악성 코드인지 혹은 정상 패킷인지를 판명한다.

그림 5는 기존의 NIDS 모델에서 IP 단편화 공격에 대해서 IDS엔진에 재조합 및 탐지모듈을 구현한 NIDS모델이다.

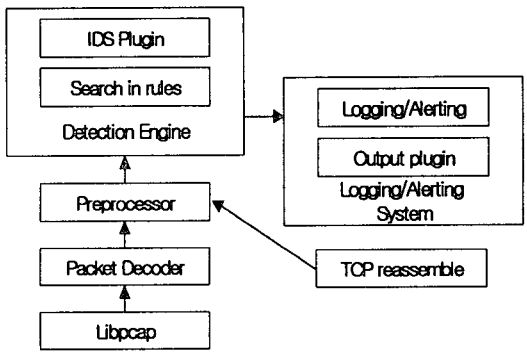

그림 6. NIDS 구성도

NIDS의 전체적인 구성도는 그림 6과 같다. Preprocessor는 일반적인 Signature Detecting이 하는 일을 보완해 주거나, 전혀 새로운 작업을 추가할 수 있게 해준다. 이 부분에 TCP 재조합 모듈을 추가한다면 보다 IP 단편화 공격에 대한 탐지를 효율적으로 할 수 있다.

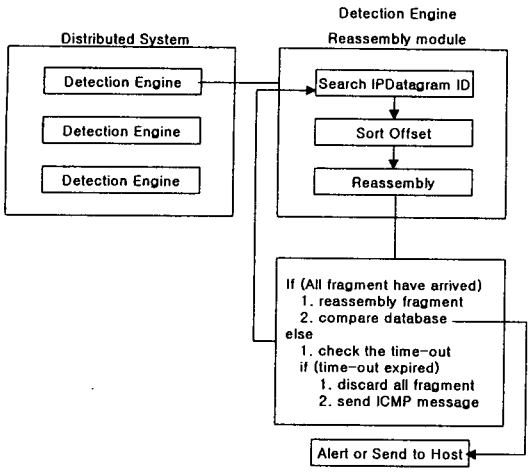

그림 7. 제안한 NIDS 모듈

그림 7은 IP 단편화 공격에 대한 모듈을 구현한 것이다. 분산 시스템에 의해서 검색엔진이 들어오는 패킷을 모두 검사를 한다. 재조합 모듈을 포함한 검색엔진은 먼저 IP 데이터그램의 ID를 검색하고 단편화 오프셋을 보고 순서를 정렬한다. 다음으로 만약에 단편화된 패킷들이 모두 들어오게 된다면 재조합 후에 데이터베이스와 비교하여 레드 코드일 경우 Alert를 하고 아닐 경우 호스트에 패킷을 전달한다. 만일 단편화된 패킷들이 모두 들어오지 않았다면 재조립테이블의 time-out 필드를 체크한 후 시간이 지났을 경우 패킷을 폐기하고 ICMP 오류 메시지를 발신지에 보낸다. 그리고 다시 첫 번째의 탐색 모듈로 돌아간다.

4. 모의실험 및 결과

그림 8은 210.110.146.218의 IP주소를 가진 호스트가 210.110.146.211의 IP주소를 가진 서버로 nmap을 이용한 Tiny 단편화 공격에 대한 탐지 결과를 보여준다.

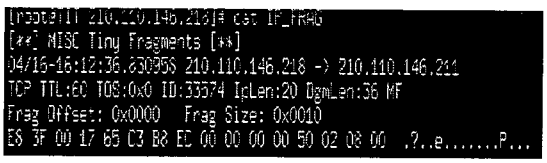

그림 8. Tiny 단편화 공격

IP 단편화 탐지 모듈은 Tiny 단편화 공격과 fragment overlap 공격 및 IP 단편화를 이용한 서비스 거부 공격 등의 모든 단편화 공격에 대해 대략 90%이상의 탐지 율을 보였다.

5. 결론

IP 단편화는 서로 다른 네트워크 환경에서 IP 패킷의 효율적인 전송을 보장해 주고 있지만 앞서 살펴본 것과 같이 몇 가지의 보안문제를 가지고 있다. 대표적인 IP 단편화를 이용한 공격은 시스템이 비정상적인 단편화를 적절히 재조합하지 못함으로써 발생되어 이로 인해 시스템이 중지되거나 재 부팅 될 수 있다. 최근에 사용하고 있는 운영체제에서는 IP 단편화를 이용한 서비스 거부 공격에 견딜 수 있도록 패치가 이미 된 경우가 많다. 하지만 서비스 거부 공격보다 최근에 더 문제가 되고 있는 것은 IP 단편화를 이용하여 침입차단 시스템이나 침입탐지시스템을 우회할 수 있는 기술이다. 제안한 침입 탐지 시스템은 호스트에 침입사실을 경고하기에 앞서 단편화된 패킷들을 재조합하여 IP 단편화를 이용한 우회 공격의 탐지가 가능하다. 하지만 네트워크 침입탐지시스템이 재 조합모듈로 인해서 호스트 자체 내의 효율저하가 발생하는 단점이 있다. 그러므로 이러한 효율저하(시간 및 고 사양 요구)를 해결하는 연구가 계속 되어야 할 것이다.

[참고문헌]

[1] http://www.certcc.or.kr

[2] Stephen Northcutt, Judy Novak "Network Intrusion Detection An Analyst's Handbook".

[3] Martin Roesch," Snort - Lightweight Intrusion Detection for Networks"

[4] James Martin, joe Leben, "TCP/IP Networking : Architecture, Adminstration, and Programming", Prenice Hall, August 1994.

[5] 유동훈, InetCop Team "실전해킹", 파워북

[6] Behrouz a. Forouzan, "TCP/IP Protocol Suite"

[7] 임채호, "중요정보통신망 해킹시 침입자기법 분석과 대응", 한국 정보보호 센터