패턴분류와 해싱기법을 이용한 침입탐지 시스템

(Intrusion Detection System using Pattern Classification with Hashing Technique)

윤 은 준* 김 현 성** 부 기 동**
(Eun-Jun Yoon, Hyun-Sung Kim, Ki-Dong Bu)

요 약 인터넷의 대중화로 인한 네트워크의 급속한 팽창으로 보안관리가 중요하게 인식되고 있다. 특히, 이상패킷을 이용한 공격들은 비정상적인 패킷들을 통하여 침입탐지 시스템이나 침입차단 시스템을 우회하여 공격하기 때문에 탐지해 내기가 어렵다. 본 논문에서는 이상패킷을 이용한 공격들을 실시간에 효율적으로 탐지할 수 있는 네트워크 기반의 침입탐지 시스템을 설계하고 구현한다. 침입탐지 시스템을 설계하기 위하여 먼저 침입 탐지를 위한 패턴을 분류하고 이를 기반으로 해싱기법이 적용된 룰트리를 생성한다. 생성된 룰트리를 기반으로 제안한 시스템은 이상패킷 공격을 효율적으로 실시간에 탐지한다.

Abstract Computer and network security has recently become a popular subject due to the explosive growth of the Internet. Especially, attacks based on malformed packet are difficult to detect because these attacks use the skill of bypassing the intrusion detection system and Firewall. This paper designs and implements a network-based intrusion detection system (NIDS) which detects intrusions with malformed-packets in real-time. First, signatures, rules in NIDS like Snorts rule files, are classified using similar properties between signatures. NIDS creates a rule tree applying hashing technique based on the classification. As a result, the system can efficiently perform intrusion detection.

1. 서 론

네트워크에 대한 부정침입이나 사이버테러의 문제가 심각해짐에 따라 최근 등장하고 있는 정보 시스템 기술이나 정보보호 시스템은 해킹에 대응할 수 있는 각종 방법을 고려하여 개발되고 있다. 그러나 이에 따른 해킹기술 또한 고도로 지능적이고 기술화되어 가고 있다. 이러한 공격기술들은 대규모 단위의 네트워크를 대상으로 하고 있으며 단 하나의 패킷으로도 네트워크 자체를 아예 정지시키거나 마비시킬 수 있는 엄청난 위력을 보이고 있다. 또한 각종 해킹 툴이나 기법들이 대중화됨에 따라 네트워크 관련 공격들이 점점 다양해지고 있고 그 중에서도 이상패킷들을 이용한 공격은 침입탐지시스템이 탐지해내기 어려운 다양한 형태와 크기로 공격하기 때문에 침입탐지 시스템을 우회하여 서비스 거부 공격을 한다거나 프로토콜 스택을 파괴함으로서 그 심각성이 매우 커지고 있다[1]. 이러한 공격들은 네트워크를 통해 전달되는 패킷들의 특성을 파악하여 분석함으로써 침입을 탐지할 수 있다[2].

침입탐지를 검사하기 위한 방법으로는 패턴매칭 방법과 인공지능 기법을 이용한 방법 및 통계적인 방법 등이 있다. 몇몇 연구 프로젝트에서 인공지능 기법이나 통계적인 방법등이 이용되지만 대부분의 상용화된

* 경북대학교 컴퓨터공학과
** 경일대학교 컴퓨터공학부

침입탐지 시스템은 패턴매칭 방법을 이용하고 있다[3,4]. 패턴매칭 방법은 알려진 공격방법을 탐지할 수 있는 일정 규칙인 패턴을 가지고 있으면서 현재 행위와 공격으로 설정된 패턴을 비교하여 침입을 탐지하는 방식이다. 패턴매칭을 통한 기존의 시스템에서는 많은 시간이 소요되어 실시간으로 침입을 탐지하기 어려운 문제점이 존재하였다[4]. 이러한 문제점을 보완하기 위한 방법으로는 공격 유형이 비슷하거나 공격간에 중복되는 특성을 이용하여 공격을 유형별로 패턴화하는 방법들이 있다[5]. 기존의 패턴매칭 기법을 이용한 침입 탐지 시스템에서는 이상 패킷을 이용한 서비스 거부 공격에 대응하지 못하는 단점이 존재한다.

본 논문에서는 이상패킷을 이용한 공격들을 실시간에 효율적으로 탐지할 수 있는 네트워크 기반의 침입탐지 시스템을 설계하고 구현한다. 침입탐지 시스템을 설계하기 위하여 먼저 침입 탐지를 위한 패턴을 분류하고 이를 기반으로 해싱기법이 적용된 룰트리를 생성한다. 생성된 룰트리를 기반으로 제안한 시스템은 이상패킷 공격을 효율적으로 실시간에 탐지한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서 이상패킷을 이용한 공격유형에 대하여 살펴본다. 3장에서는 이상패킷을 효율적으로 탐지할 수 있는 네트워크 기반의 침입탐지시스템을 설계한다. 4장에서는 설계한 시스템의 시뮬레이션 결과를 제시하고 마지막으로 5장에서 결론 및 향후연구에 대하여 기술한다.

2. 공격유형

침입탐지시스템은 여러 가지 기준에 의해서 분류되는데 크게 데이터 소스 기반이 네트워크 패킷인 네트워크 기반의 침입탐지 시스템과 호스트에서 발생하는 이벤트에 기반을 둔 호스트 기반의 침입탐지 시스템의 두 가지 형태가 있다. 본 논문에서는 데이터 소스 기반을 네트워크 패킷으로 연구를 한정한다.

본 장에서는 시스템의 보다 효율적인 이해를 위하여 이상 패킷을 이용한 서비스 거부 공격과 침입탐지 시스템을 우회하는 공격 유형에 대해서만 살펴본다. 먼저 서비스 거부 공격은 사람의 시간과 네트워크의 대역폭을 낭비하는 것 이외에도 조금씩 시스템에 해를 끼치며 때때로 시스템을 다운시키기도 한다. 이러한 공격들은 대부분 무차별한 서비스 거부 공격 형태로 이루어진다. 그러나 좀더 세련된 형태의 공격은 단지 하나의 위조된 패킷을 이용하여 시스템을 다운시키게 하는 공격도 있다[6]. 서비스 거부 공격의 유형은 다음과 같다.

Ping of Death, Jolt : 이 공격은 패킷 단편의 취약점이나 서비스 거부 공격을 이용한 공격 방법이다. 일반적으로 ping은 ICMP 메시지 타입 중 echo 요청과 echo 응답을 이용한다. 이러한 ping을 이용한 공격은 가장 손쉽게 IP 패킷을 전송 할 수 있는 공격 방법으로서 ICMP echo 요청 패킷을 상대방에게 전송한다. 이때 공격 패킷은 표준에 규정된 길이(65,535) 이상으로 큰 IP 패킷을 전송함으로써 이 패킷을 수신받은 시스템에서 이 비정상 패킷을 처리하지 못하게 함으로써 서비스 거부 공격이 발생되도록 하는 방법이다.

Teardrop, Bonk, New Teardrop : Teardrop 공격은 단편(Fragment)의 재조합 과정의 취약점을 이용한 서비스 거부 공격으로, 서로 중첩되도록 헤더를 조작한 한 쌍의 IP 패킷조각들의 재조합 과정에서 내부 버퍼를 넘치게 함으로써 수행된다. 이 과정에서 버퍼에 복사해 넣어야 할 데이터의 길이 값이 음수가 되게 되고 이것을 여러 번 반복하면 시스템이 정지되거나 재부팅 된다.

Land Attack : 이 공격은 TCP 연결 요청 패킷인 SYN 패킷 헤더의 발신자 주소 및 포트번호를 조작하여 전송함으로써 네트워크 자원을 낭비시키거나 시스템의 실행 속도를 현저히 저하시킨다. Land Attack은 TCP 연결 요청 패킷인 SYN 패킷 헤더의 발신자 IP주소와 접속포트의 값을 공격대상 시스템의 IP주소와 포트로 설정하여 공격대상 시스템에 보낸다. 이 패킷을 수신한 시스템은 이 요구가 자기 자신으로부터 발송된 연결요청인 것으로 받아들여 자신에게 계속적인 응답 패킷을 보내게 되며, 결국에는 시스템이 불완전한 연결설정 상태에 빠지게 된다.

대부분의 침입탐지시스템에서 사용하는 침입탐지는 패턴매칭기법에 기반하기 때문에 공격자들은 공격을 숨기기 위하여 침입탐지 시스템에서 검사되는 패턴이 아닌 것처럼 공격 데이터를 변조하여 탐지를 피한다. 또는 네트워크 기반의 침입탐지 시스템들은 패킷 재조합 기능을 제공하지 못하기 때문에 패킷 단편화를

통하여 탐지를 피할 수 있다[7,8]. 침입탐지 시스템 우회 공격의 유형은 다음과 같다.

미세한 단편 공격 (Tiny Fragment Attack) : 이 공격은 최초의 단편을 아주 작게 만들어서 네트워크 침입탐지시스템이나 패킷 필터링 장비를 우회하는 공격이다. 예를 들어 TCP 헤더(일반적으로 20바이트)를 2개의 단편으로 나뉘어질 정도로 작게 쪼개서 목적지 TCP 포트번호가 첫 번째 단편에 위치하지 않고 두 번째 단편에 위치하도록 한다. 패킷 필터링 장비나 침입탐지시스템은 필터링을 위해 포트번호를 확인하는데, 이를 피하기 위하여 공격자는 포트번호가 포함되지 않을 정도로 아주 작게 단편된 첫 번째 단편을 통과시킨다. 또한 포트번호가 포함되어 있는 두 번째 단편은 침입탐지시스템으로부터 아무런 검사 없이 통과한다. 그 결과 보호되어야 할 목적지 서버에서는 이 패킷들이 재조합되고 공격자가 원하는 포트를 통해 공격할 수 있다.

단편 겹치기 공격 (Fragment Overlap Attack) : 이 공격은 미세한 단편 공격기법에 비해 좀더 정교한 공격이다. 공격자는 공격용 IP 패킷을 위해 두 개의 단편을 생성한다. 첫 번째 단편은 패킷 필터링 장비에서 허용하는 HTTP(TCP 80) 포트와 같은 포트번호를 가진다. 그리고, 두 번째 단편에서는 오프셋(Offset)을 아주 작게 조작해서 단편들이 재조합될 때 두 번째 단편이 첫 번째 단편의 일부분을 덮어쓰도록 한다(Overlap). 일반적으로 공격자들은 두 번째 단편의 오프셋을 이용하여 첫 번째 단편의 포트번호가 있는 부분까지 덮어쓴다.

비정상적인 TCP 플래그 : TCP 프로토콜은 연결의 상태나 패킷의 우선순위 등을 나타내는 다양한 플래그를 사용한다. 많은 공격 패킷들이 이러한 TCP 플래그들을 조작하여 수행된다. 이렇게 불법 조작된 패킷들을 통하여 공격자는 공격하고자 하는 네트워크나 서버를 탐색하고 파괴시킬 수 있다. 뿐만 아니라 이러한 TCP플래그의 조작된 패킷들은 침입차단시스템이나 침입탐지시스템에 의한 패킷탐지를 어렵게 만든다.

3. 침입탐지 시스템

본 장에서는 이상패킷을 이용한 공격들을 실시간에 효율적으로 탐지할 수 있는 네트워크 기반의 침입탐지 시스템을 설계하고 구현한다. 시스템구성을 위하여 먼저 다양한 공격 패턴들을 분류하고 그 분류에 따라 공격을 탐지할 수 있는 침입탐지 모듈을 설계한다. 시스템은 패턴분류와 침입탐지 모듈에 초점을 맞추어 설명하고자 한다. 이 장에서는 먼저 제안한 시스템의 구성요소에 대해 살펴보고, 2장에서 언급한 공격 유형에 대한 탐지 방법을 예제로 하여 공격 유형을 분류하고 이에 대응하는 해싱기법이 적용된 룰트리를 생성하고 공격을 탐지하는 방법에 대해서 살펴본다.

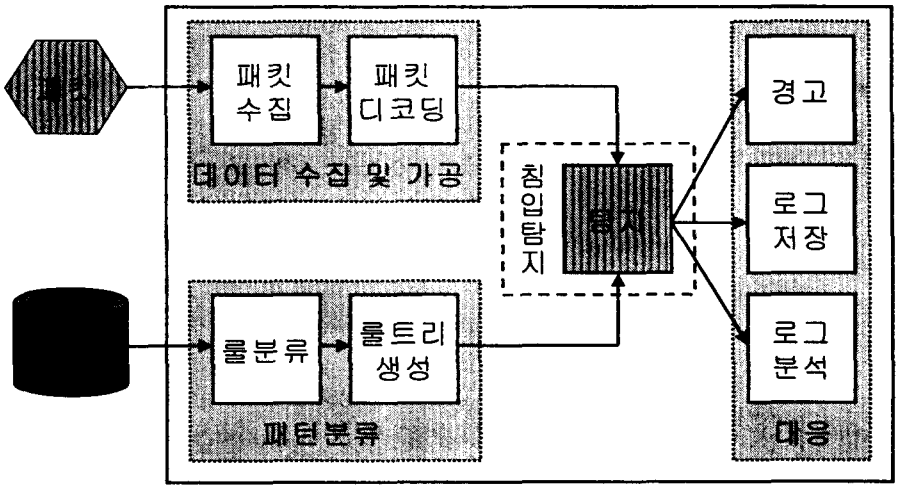


그림 1. 침입탐지 시스템

3.1. 시스템 구성

네트워크 기반의 실시간 침입탐지 시스템의 구성은 그림 1과 같다. 이 시스템은 다음과 같이 4가지 단계로 구성되며 각 역할은 다음과 같다.

- 패킷수집 및 가공 : 네트워크 패킷 수집 및 데이터 가공
- 패턴분류 : 분류된 패턴에 따른 룰트리 생성
- 침입탐지 : 룰트리를 통한 침입여부 판단
- 대응 : 로그를 작성하고 관리자에게 경고

패킷수집 및 가공 모듈에서는 패킷 수집을 위하여 리눅스에서 기본적으로 제공하는 BFP 드라이버를 사용하고, 수집된 패킷을 적절히 필터링 하기 위하여 LibPcap 라이브러리[9]를 사용한다. 패턴분류 모듈과 침입탐지 모듈에 대해서는 다음절에서 상세히 다룬다. 대응모듈에서는 원시데이터와 분석된 패킷관련 정보를 추후에 이용하기 위하여 데이터베이스에 저장한다. 또한 침입탐지 모듈에서 제공된 분석정보를 기반으로 침입의 레벨에 따라 적절한 대응을 수행하고, 보안담당자에게 해당 정보를 알려준다.

3.2. 공격유형에 따른 침입 패턴 분류

본 절에서는 이상 패킷과 관련된 헤더정보를 성능과 효율성을 고려하여 실시간으로 침입여부를 분석할 수 있는 방법을 제시한다. 침입탐지 모듈에서는 먼저 표 1에서 제시된 공격 유형에 따라 분석된 패턴을 이용하여 1차로 침입여부를 확인한 후 TCP 플래그 검사 및 IP 단편 필터링과 같은 약간의 축적된 정보를 요구하는 분석을 수행한다.

가. 발신지와 수신지의 주소와 포트 검사

발신지의 IP 주소와 포트번호는 서비스 거부 공격이나 스캐닝 공격 등을 탐지할 때 중요하게 사용된다. 대부분의 공격에서는 IP의 출발지 주소값을 모두 거짓으로 채워 보내므로 공격지를 찾기는 매우 힘들고 이를 정확하게 탐지하기도 힘들다. 하지만 발신지와 수신지의 IP주소와 포트번호(사용 서비스)를 자세히 분석하여 그 부담을 줄일 수 있다. 다음은 주소와 포트를 기반으로 한 침입탐지 규칙이다.

- 발신지의 주소와 수신지의 주소가 같은지 검사한다.
- 임의의 호스트로부터 보안에 취약한 특성을 갖는 서비스 혹은 포트에 대한 사용을 탐지한다.
- 특정 목적지 호스트나 네트워크로의 접근 시도를 탐지한다.

표 1. 공격유형에 따른 패턴분류

Size Checking	IP total length가 표준에 규정된 적당한 길이인지 검사	Ping of Death, Jolt
	TCP/IP header length가 유효한 범위내에 있는지 검사	Tiny Fragmentation Attack
IP Fragmentation	첫번째 패킷과 겹치는 오프셋이 있는지 검사	Teardrop, Fragment Overlap Attack
TCP Flag	SYN, FIN 동시수행패킷	Stealth Scan, Network Mapping, Portscan
	FIN 단독 플래그	
	NULL / XMAS 플래그	
	ACK 번호 == 0	
	SYN 연결에 데이터가 포함여부	
Address/Port Checking	발신지와 수신지의 주소와 포트번호가 같은지 검사	Land Attack

나. 패킷 헤더 길이 검사

서비스 거부 공격 방법 중에는 일부 프로토콜에서 사용되는 패킷의 크기를 조작하여 버퍼를 넘치게 함으로서 시스템의 오류를 일으키거나 불충분한 정보로

인해 침입탐지시스템을 우회하는 공격방법이 있다. 이러한 공격을 탐지하기 위해서는 IP와 TCP의 헤더길이가 표준에 규정된 길이의 범위에 있는지를 검사한다.

다. TCP 플래그 검사

TCP 플래그 검사를 위해서는 자주 발생되는 비정상적인 플래그들의 유형을 조사하여 패턴을 정해 놓는다[10,11]. 그리고 그 패턴과 비교하여 위배되는 패킷을 탐지하여 경고하도록 설정함으로써 악성의 공격 및 활동들을 탐지할 수 있다. 다음은 플래그별 공격유형이다.

- **SYN, FIN 플래그** : SYN, FIN을 동시에 수행하는 정상적인 패킷은 없다. 이외에도 SYN FIN PSH, SYN FIN RST, SYN FIN RST RSH 와 같은 SYN FIN들의 다양한 변형들이 존재한다.
- **FIN 플래그** : 정상적인 TCP세션 연결을 종료하고 싶을 경우, 클라이언트나 서버 중 하나의 호스트에서 FIN신호를 보냄으로써 수행된다. 그러므로 FIN플래그가 켜져 있다는 것은 그전에 두 호스트간에 3방향 핸드쉐이크가 수행되었다는 것을 의미한다. 그러나 3방향 핸드쉐이크가 시작된 적이 없는 곳에 FIN 플래그가 설정되어 있다면 이는 정상적인 패킷이 아니다. 이러한 FIN 패킷들은 주로 포트스캔, 네트워크 매핑, 스텔스 스캔 등을 하기 위하여 사용된다.
- **NULL** : 어떤 플래그도 설정되지 않은 패킷을 말한다.
- **XMAS** : 플래그가 모두 설정되어 있는 패킷을 말한다.
- **ACK번호 == 0** : ACK 플래그가 켜져 있는 TCP 세그먼트는 3방향 핸드쉐이크시에 생성되는 최소 응답확인 값이 1이어야 한다.
- **SYN 연결에 포함된 데이터의 탐지** : SYN만 설정된 패킷은 새로운 연결을 시도할 때만 사용되기 때문에 어떤 데이터도 포함하지 않는다.

라. IP 단편 필터링

IP 단편을 이용한 우회공격을 탐지하기 위해서 침입탐지시스템은 단편화된 패킷들을 재조합할 수 있어야 한다. 하지만 네트워크 침입탐지시스템이 단편된 패킷을 재조합하기 위해서는 메모리나 프로세스 등 많은 시스템 자원을 필요로 하므로 실시간 탐지가 어렵다는 문제가 있다[8]. 본 논문에서 제안한 침입탐지시스템은 패킷을 검사하는 과정에서 본 논문에서 제안한 단편필터링 알고리즘을 이용하여 단편화된 패킷 공격을 실시간으로 탐지할 수 있다.

필터링 알고리즘은 첫 번째 패킷의 단편과 관련된 헤더정보인 ID(Identification), 헤더길이(Header Length), 전체길이(Total Length), 두 번째 패킷의 오프셋, 출발지 주소(Source Address), 목적지 주소(Destination Address)를 자료구조에 저장한다. 패킷들은 다양한 경로들을 통해 들어오기 때문에 모든 단편들을 필터링하여 저장하기는 힘들다. 그러나 다행히도 중요한 패킷의 정보는 헤더의 시작부분에 포함하기 때문에 첫 번째 단편과 두 번째 단편만을 필터링 하면 된다[12]. MF 플래그가 켜져 있는 최초의 단편(오프셋 == 0)이 도착하면 링크드 리스트(Linked List)로 구성된 자료구조의 ID항목에 단편의 헤더정보를 기록하고 오프셋이 0이 아닌 패킷이 들어왔을 때 동일한 ID를 매칭하여 두 번째 패킷의 오프셋을 기록한다. 그리고 첫 번째 패킷의 헤더 전체길이와 비교하여 겹치는 부분이 있는지 확인한다. 겹치는 부분이 있다면 단편 겹치기 공격으로 간주하고 적절한 대응을 수행한다. 버퍼 오버플로우(Buffer Overflow)를 방지하기 위하여 패킷들 간의 전송되는 시간 간격을 측정하여 두 번째 패킷 전송후 일정시간이 소요된 패킷은 버퍼에서 삭제한다. IP 단편 필터링 알고리즘은 다음과 같다.

```
단편 필터링 알고리즘 {
  if (flag == MF && offset == 0) {
     패킷의 ID, 오프셋, 전체길이를 저장 ;
  }
  else if (flag == MF && 오프셋 != 0) {
      ID를 검색하여 동일한 것을 찾음 ;
       if (두 번째 패킷 오프셋 == null) {
         if ((전체길이/8) > 오프셋) {
            alert 하고 버퍼에서 삭제 ;
         }
```

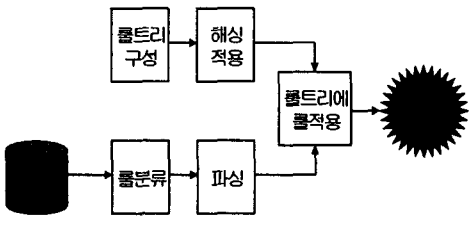


그림 2. 룰트리 생성과정

```
        else
            오프셋 최소값으로 저장 ;
        }
        else if (두 번째 패킷 오프셋 != null) {
          if (최소값 > 현재 오프셋) {
            if ((전체길이/8) > 오프셋) {
              alert 하고 버퍼에서 삭제 ;
                }
            else
              현재 오프셋을 최소값으로 저장
;
            }
        }
    }
}
```

3.3. 룰트리

공격을 효율적으로 탐지하기 위하여 3.2절에서 분류된 방법이 적용된 침입을 탐지하기 위하여 본 시스템에서는 룰트리를 이용한다. 그림2는 침입탐지 모듈에서 사용될 룰트리 생성과정을 보여준다.

효율적인 룰 적용을 위하여 본 시스템에서는 정형화된 공개침입탐지 시스템인 Snort의 룰 파일을 입력으로 한다. Tiny Fragments 공격을 탐지하기 위한 Snort 룰의 한 예는 다음과 같다.

```
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"MISC Tiny Fragments"; fragbits:M; dsize: < 25; classtype:bad-unknown; sid:522; rev:1;)
```

룰 헤더에는 어떤 패킷인가, 어디서 온 것인가에 관한 정보가 있고, 그에 따른 이벤트도 이곳에 정의 되어있다[3]. 제안한 시스템의 룰트리를 만들기 위해서는 그림 2의 절차와 같이 Snort의 룰을 입력으로 하여 표 1에서 제시한 공격유형에 따른 패턴분류를 통하여 룰을 분류한다. 그리고, Snort의 룰을 입력으로 한 룰트리를 생성한다. 이러한 룰트리를 생성하는 과정에서 탐색의 효율을 증대시키기 위하여 고정된 값을 가진 트리의 노드에 해싱(Hashing) 기법을 적용한다. 예를들어 IP나 포트에 mod 20의 해싱을 적용할 수 있다. 이러한 해시 함수는 시스템에 따라서 다르게 적용할 수 있다. 룰트리 생성과정에서 이러한 해싱 기법을 적용함으로서 시스템에서 침입탐지시 보다 효율적인 탐색을 제공할 수 있다.

4. 시뮬레이션

제안한 시스템을 시뮬레이션하기 위한 환경은 다음과 같다.

- 시스템 사양 : Intel Pentium-III 1GHz, 128M
- 운영체제 : Linux Kernel 2.4.7
- 패킷수집 : LibPcap 0.6.2
- 공격툴 : 공격용 해킹툴인 Teardrop과 Nmap 및 다양한 이상패킷을 이용한 공격툴

시뮬레이션을 위하여 위에 언급한 시스템 사양의 컴퓨터 10대를 이용해서 환경을 구성하였다. 내부 네트워크 환경을 위하여 다섯대의 컴퓨터가 사용되었고, 침입탐지 시스템을 위한 하나의 컴퓨터, 그리고 나머지 네 대의 컴퓨터를 이용하여 공격 시나리오를 작성하였다. 제안한 시스템의 성능 평가를 위하여 이상패킷을 이용한 여러 가지 형태의 해킹툴을 가지고 다양한 조건에서 공격을 시도해 보고 탐지율을 조사하였다.

다양한 공격유형으로 공격한 결과 모두 False-Positive 오류율 0%에 탐지율 100%의 결과를 보였다. 또한 단편을 이용한 서비스 거부공격을 효율적으로 탐지할 수 있음을 확인하였고, 이러한 특성은 잘 알려진 네트워크 침입탐지 시스템인 Snort와 견줄만하다.

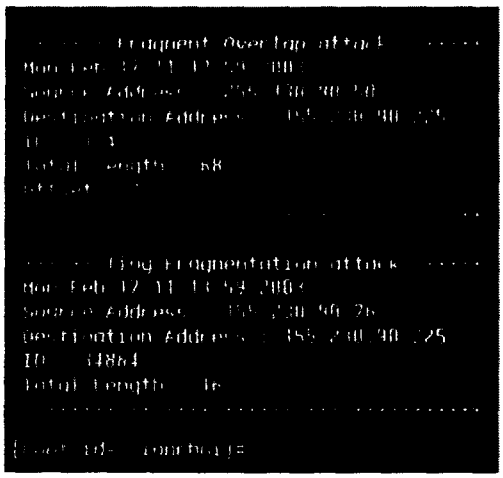


그림 3. IP 단편 필터링을 통한 탐지 결과

표 2. 침입탐지 시스템의 탐지율

공격유형	탐지율
Ping of Dearth, Jolt	100%
Tiny Fragmentation Attack	100%
Teardrop, Fragment Overlap Attack	100%
Stealth Scan, Network Mapping, Portscan	100%
Land Attack	100%

그림 3은 단편겹치기 공격과 미세한 단편 공격을 동시에 수행했을 때의 침입결과를 보여준다.

5. 결론 및 향후연구

네트워크 상에 있는 컴퓨터 시스템에 대한 침입 행위들은 끊임없이 새롭게 개발되고 패턴의 변화가 다양해짐에 따라 이에 대한 효율적이고 빠른 침입 탐지 방법이 필요하다. 특히 이상패킷을 이용한 공격들은 비정상적인 패킷들을 통하여 서비스 거부 공격을 하거나 패킷 필터링 장비나 침입차단시스템을 우회하기 때문에 탐지해 내기가 어렵다. 본 논문에서는 실시간에 효율적으로 이상패킷을 이용한 공격을 탐지해 낼 수 있는 네트워크 기반의 침입탐지 시스템을 설계하고 구현하였다. 효율적인 시스템을 구성하기 위하여 먼저 침입의 유형별 패턴을 분류하여 효율적인 자료구조의 해싱이 적용된 룰트리를 구성하였다. 제안한 시스템의 실험결과는 False-positive 오류율이 0%였고 탐지율이 100%임을 보였다.

향후 연구 과제로는 현재의 시스템을 보다 최적화 시키고, 이상 패킷을 이용한 공격 뿐 만 아니라 보다 다양한 공격에 대응할 수 있는 시스템을 구축하는데 있다. 또한, 새로운 공격이 발견되었을 때 그러한 공격을 시스템이 효율적으로 탐지할 수 있도록 새로운 패턴의 효율적인 업데이트에 관한 연구가 필요하다.

참 고 문 헌

[1] Paul E. Proctor, Practical Intrusion Detection Handbook, Prentice Hall PTR, 2001.

[2] Marina Bykova, Shawn Ostermann, Brett Tjaden, "Detection Network Intrusions via Statistical Analysis of Network Packet Characteristics", 33rd Southeastern Symposium on System Theory (SSST) , 2001.

[3] The Open Source Network Intrusion Detection System, "http://www.snort.org

[4] 한국정보보호진흥원,"http://www.kisa.or. kr

[5] 강창구, 김주영외. 네트워크 패킷 분석을 통한 침입탐지 기법 개발, 한남대학교 컴퓨터공학과 논문지. pp. 1-7.

[6] Stephen Northcut, Judy Novak, Network Intrusion Detection An Analyst's Handbook Second Edition, New Riders, 2001.

[7] Ed Skoudis, Counter Hack, Prentice Hall PTR, 2002.

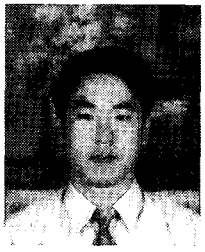
[8] 정현철, IP Fragmentation을 이용한 공격기술들, 한국 정보보호 센터, 2001.

[9] Libpcap library, "ftp://ftp.ee.lbl.gov/ libpcap.tar.Z"

[10] 김상철, Abnormal IP Packets, 해킹바이러스 상담지원 센터, 2001.

[11] Thomas H. Ptacek , Timothy N. Newsham, "Insertion, Evasion, and Denial of Service : Eluding Network Intrusion Detection", Technical Report, Secure Networks Inc., 1998.

[12] Ziemba, Reed & Traina, "Security Considerations for IP Fragment Filtering", RFC1858, 1995.



윤 은 준 (Eun-Jun Yoon)

1995년 2월 : 경일대학교 섬유패션학과 공학사

2003년 2월 : 경일대학교 대학원 컴퓨터공학과 공학석사

2003년 3월~현재 : 경북대학교 컴퓨터공학과 박사 과정

관심분야 : 보안기술, 정보보호 응용기술

김 현 성 (Hyun-Sung Kim)

1996년 2월 경일대학교
컴퓨터공학과 공학사
1998년 2월 경북대학교
컴퓨터공학과 공학석사
2002년 2월 경북대학교
컴퓨터공학과 공학박사
2002년 3월~현재 경일대학교 컴퓨터공학과 교수
관심분야 : 정보보안, 암호 알고리즘, 암호 프로세서 설계, IDS, PKI

부 기 동 (Ki-Dong Bu)

1984년 경북대학교 전자
공학과 전자계산기 전공
1988년 경북대학교 대학원
전산공학전공 공학석사
1996년 경북대학교 대학원
전산공학전공 공학박사
1983년~1985년 포항종합제철 시스템개발실
2001년 9월~2002년 8월 게이오대학 교환교수
1988년~현재 경일대학교 컴퓨터공학과 교수
관심분야 : 데이터베이스, GIS, 시멘틱 웹