패킷 순차성을 이용한 비정상행위 침입 탐지

홍동호*, 유황빈*

*광운대학교, 컴퓨터 과학과

Anomaly Intrusion Detecion Using Sequential Properties of Packets

Dong-ho Hong*, Hwang-bin Ryou*

*Department of Computer Science, Kwangwoon Univ.

요 약

인터넷 상에서의 대부분의 네트워크 공격은 공격의 목표가 되는 시스템에 단일 패킷만을 보냄으로써 공격이 이뤄질 수 없다. 그렇기 때문에 침입탐지시스템에서는 내부 네트워크로 들어오고 나가는 패킷들에 대한 일련의 순차성을 알아냄으로써 네트워크 공격을 탐지할 수 있다. 본 연구에서는 이러한 네트워크 패킷의 순차성을 이용하여 비정상행위에 대한 침입탐지 방법을 제안하였으며 또한 일부 비정상행위 탐지에서 사용하고 있는 시간을 기준으로 한 트랜잭션의 분할에서 오는 단점을 지적하고 그것을 보완하기 위하여 탐지 단위로서 사용자의 세션을 사용하였다. TCP/IP 네트워크에서의 사용자 세션 정보를 표현하기 위해서 여러 가지 정보가 사용자 행위 테이블로 표현되며 이러한 사용자 행위 테이블은 서비스 포트 별로 통계적인 정리가 가능하다. 또한 이렇게 정리된 서비스 포트별 정보에서는 확률을 기반으로 한 비정상 행위를 도출할 수 있으며, 이러한 비정상 행위도를 이용하여 침입 판단의 근거자료로 삼을 수 있음을 확인하였다.

I. 서론

컴퓨터와 초고속 인터넷의 보급으로 인하여 정보화 사회로 접어든 것은 사실이지만, 이에 반해 정보에 대한 위협이 증가하게 되었다. 해킹이나 바이러스에 대한 피해 신고는 2002년 15,192건에서, 2003년 6월 현재 지난해의 피해수가 초과된 16,055건으로 확인되었다. 또한 공격에 대한 표적이 대형화되며, 날이 갈수록 공격 기법이 고도화되가는 특징을 가지고 있다. 최근 발생한 인터넷 침해 사고를 보자면 분산 서비스 공격과 각종 웜 바이러스 공격이 주를 이루고 있다. 지난 1.25 인터넷 대란은 슬래머 웜이라고 불리는 바이러스로 인해 네트워크 트래픽을 증가시켜 사상 초유의 인터넷 마비를 일으켜, 전 세계적으로 엄청난 피해를 입혔다. 그렇기 때문에 이러한 인터넷 공격에 대한 탐지와 대응이 그 피해를 최소 할 수 있는 방법이라고 할 수 있다.

현재까지 개발된 침입탐지시스템은 대부분 오용 탐지 기법을 이용하고 있다. 오용 탐지 기법은 공격 탐지의 정확성이 높다는 장점을 가지고 있지만, 새로운 공격에 대한 탐지는 거의 불가능하다는 큰 단점을 지니고 있다. 반면 비정상행위 침입 탐지 기법은 정상과 비정상의 판단이 어렵고 높은 오판율을 가지고 있지만, 새로운 공격에 대한 탐지가 가능하기 때문에 근래에 많이 연구되고 있는 분야이다. 비정상행위 침입탐지 기법에도 여러 가지 방법이 있으나 통계적 방법, 데이터 마이닝등이 가장 많이 연구되고 있다. 통계적 방법은 과거의 경험적 자료를 토대로 탐지하기 때문에 비교적 정확한 탐지 성능을 가지고 있지만, 어떤 행위에 대한 발생 순서에는 민감하지 못하고 모델링 할 수 있는 침입 탐지의 종류가 제한적이라는 단점을 가지고 있다. 그리고 데이터 마이닝은 침입 탐지를 하기 위해서 시간 단위의 트랜잭션을 처리하기 때문에 침입 탐지의 단절이라는 단점이 있다. 위와 같은 비정상행위 탐지방법들은 시간 단위의 탐지 구간을 설정하기 때문에 공격 탐지에 대한 단절이 이루어질 수 있고, 따라서 적절한 공격 탐지에 방해가 될 수 있다.

본 연구에서는 이러한 단점을 보완하기 위해서 네트워크 세션을 침입 탐지의 단위로 사용하였

다. 연결 지향 프로토콜에서는 사용자의 행위 파악을 위해 연결 세션별 정보를 저장하고 있는 사용자 행위 테이블을 생성하였으며 이 테이블은 TCP 연결 과정, TCP 연결 해제 과정의 2단계로 나뉘어 정보가 저장되며 각 세션내에서의 통계적 자료를 이용하여 서비스 포트에 대한 임계치가 결정되어 침입 판단에 대한 유용한 자료로 쓰인다. 위와 같은 실험을 하기 위하여 본 연구에서는 1999년 DARPA 데이터 셋을 이용하였다. [1]

II. 관련 연구

1. 침입의 정의와 종류

침입이란 권한을 부여받지 않은 사용자가 시스템의 자원에 접근하여 그것의 비밀성, 무결성, 가용성을 침해하는 단일 또는 일련의 보안 사건을 의미한다. 침입의 예로는 불법적인 관리자의 권한 취득, 시스템 서비스로의 공격이나 서비스의 사용을 불가능하게 하는 공격, 백도어를 설치하는 일, 바이러스의 전파, 시스템의 취약성을 부당하게 사용하는 행위등을 들을 수 있으며 또한 국제표준화기구(ISO)에서는 계획적이거나 우연하게 IT시스템으로부터 권한이 없는 사용자의 접근 또는 행위를 침입(Intrusion)으로 정의하였다. 침입에 대한 정의는 여러 가지가 있으나 일반적으로는 위에서 언급한 3가지 보안 요소에 가해를 하는 일련의 행위를 침입이라고 할 수 있다[2].

2. 침입 탐지 방법

침입을 탐지하기 위한 방법은 크게 두 가지 종류가 있다.

1) 오용탐지 기법

오용 탐지 방법은 침입에 대한 알려진 패턴 또는 시스템의 취약점을 리스트 혹은 데이터 베이스화 하고 이를 이용하여 침입임을 탐지하는 방법이다. 다음은 오용 탐지의 대표적인 기법들을 간단히 소개한 것이다.

- Signature Analysis : 공격 명세를 의미론적 수준(Semantic level)으로 표현하여 Snort와 같은 경량의 침입탐지 시스템에 사용된 기법이다.[3]

- Expert Systems : 미리 룰셋으로 공격을 명시해 놓고, 감사 이벤트와 비교하여 침입을 탐지하는 방법이다.

- State-Transition Analysis : 상태 전이를 이용하여 각종 공격을 표현한 것으로서 다양한 침입탐지시스템에 사용되었다.[4][5]

- Petri-nets : 복잡한 Signature를 쉽게 표현하여 개념적으로 단순화하고, 그래픽한 표현이 가능한 침입탐지 방법이다.

이러한 오용 탐지의 장점은 알려진 침입에 대한 패턴을 미리 저장하였다가 미래에 이러한 침입이 발생하였을때 효과적이면서 능률적으로 탐지를 할 수 있다는 데 있지만, 알려진 침입 패턴을 시스템에 수동 혹은 자동으로 입력을 해야 한다는 비용적인 문제와, 새로운 공격에 대한 탐지가 거의 불가능 하다는 성능적인 문제를 가지고 있다. 근래의 네트워크 공격의 형태가 새로운 형태가 많고, 변종이 증가하고 있는 면에서 볼때, 오용탐지 방법만으로는 효율적인 침입 탐지를 해낼수 없다는 한계점을 지니고 있다.

2) 비정상행위 탐지기법

비정상행위란 시스템이나 시스템의 자원에 대한 정상적이지 않은 사용을 함으로써 침입을 행하는 것이다. 이러한 침입 행위를 판단하는 것이 비정상행위 탐지 방법인데, 이것은 오용 탐지 방법과는 달리 정상 행위에 대한 프로파일을 근거로 침입 여부를 판단하며 사용자의 행위도가 프로파일에 표현된 정도를 넘어서게 되면 침입으로 판단하게 된다.

- Statistic : 비정상행위 침입탐지 방법 중 가장 많이 사용되고 있는 방법으로 탐지하고자 하는 변수에 대하여 그 변수의 통계정보를 이용하여 탐지하는 방법으로 IDES나 NIDES에서 사용한 바 있다.[6]

- Expert Systems : 정상적인 사용자의 사용 패턴을 룰셋으로 표현하여 그것을 통계적으로 표현하여 침입을 탐지하는 방법이다.

- Data Mining : meta learning이나 연관규칙 등의 데이터 마이닝 방법으로 시스템의 공통적 규칙을 찾아내는 방법을 사용하며 비정상행위 침입탐지 방법에 있어 근래에 가장 연구가 활발히 진행되고 있는 분야이다.

- Computer Immunology : Forrest가 제안한 방식으로서 시스템 콜의 순차성을 기반으로 정상 행위를 프로파일하는 탐지 기법이다. 위와 같은 비정상행위 탐지 방법은 정상/비정상의 판단이 난해하고 오판율이 높으며, 프로파일을 주기적으로 학습시켜줘야 한다는 단점이 있지만, 내/외부의 공격을 구분없이 탐지 가능하고 특히 알려지지 않은 새로운 공격의 탐지가 가능하다는 장점이 있다.

III. 패킷 순차성을 이용한 비정상 행위 침입탐지

1. 패킷 순차성의 의미

네트워크 공격시 공격의 대부분은 단일한 패킷만으로 구성되지 않는다. 공격이 이루어지기까지의 네트워크 패킷들은 단일한 이벤트로서 특정 순서를 가지게 된다. 패킷 순차성이란 공격뿐만 아니라 정상적인 네트워크 상황에서도 순차적인 패킷들의 이벤트 조합을 의미한다. 예를 들어 TCP 연결 설정 과정에서 TCP 제어 플래그에 대한 순차적인 성질을 서버 측에서 본다면 'SYN(j) 수신 ■ SYN(k),ACK(j+1) 송신 ■ ACK(k+1)수신' 의 단계를 거쳐 정상적인 연결이 이루어 질 것이다. 즉, 연결지향성 프로토콜에서 정상적인 네트워크 상황에서는 단일한 패킷이 갖는 의미보다 패킷들이 조합되어 일련의 의미있는 행위를 하게 된다. 이것은 정상적인 상황뿐 만 아니라 공격을 포함하는 비정상적인 상황에서도 마찬가지이다.

2. 순차성 탐지시스템의 개요 및 설계

1) 순차성 탐지 시스템의 구조

순차성 탐지 시스템의 Training Mode에서는 정상 데이터 만을 취급하여 프로파일을 생성하고, 테스팅 모드에서는 실험 데이터(공격 데이터 + 정상 데이터)를 처리하여 그 결과를 정상데이터의 프로파일과 비교 분석하여 침입임을 판단하게 된다. 그림1은 순차성 탐지 시스템의 구조도이다. 본 시스템은 앞에서도 언급하였듯이 두가지 모드로 동작하게 된다. 그 첫 번째가 Training Mode로서 정상 데이터에 대한 프로파일을 생성하기 위해 동작한다. 데이터 전처리 모듈에서는 공격이 없는 정상적인 원시데이터(tcpdumped file)를 이용하여 공격 탐지에 필요한 요소만으로 구성된 데이터(전처리된 데이터)를 생성하게 된다. 이렇게 생성된 데이터는 프로파일 생성 모듈을 통하여 세션의 정상적인 행위에 대한 프로파일(세션 행위 프로파일)을 생성하게 된다. 여기에서는 TCP 연결 설정 단계와 연결 해제 단계의 2가지 단계로 구분해서 순차 패턴을 찾아내게 된다. 그 후에 세션 행위 프로파일은 프로파일 정보화 모듈을 통하여 통계적 방법을 이용하여 서비스 포트별로 프로파일(서비스 포트별 행위 프로파일)을 생성하게 된다.

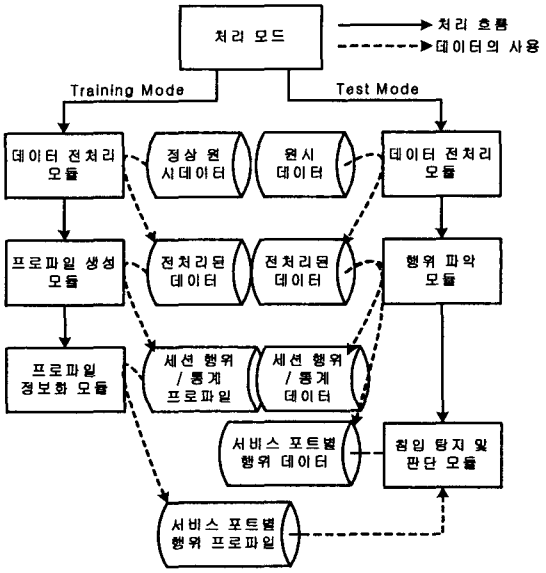

그림 1 순차성 탐지 시스템의 구조

위와같이 Training Mode의 처리 결과는 서비스 포트별로 생성된 정상행위 프로파일이 된다. 두 번째로 Test Mode가 있는데 이것의 첫 번째 단계는 Training Mode에서 그것과 마찬가지로 침입 탐지에 필요한 요소로만 구성된 데이터를 생성하는 데이터 전처리 모듈이며, 단지 여기에서는 공격이 없는 데이터가 아닌 공격이 포함된 실험 데이터를 이용하게 된다. 다음으로 행위 파악 모듈에서는 전처리 된 데이터를 이용하여 TCP 연결 설정 단계와 연결 해제 단계의 2가지 단계로 구분해서 사용자의 행위 파악을 하게 된다. 그 결과는 세션 행위 데이터와 서비스 포트별 행위 데이터로 저장되며 이것은 침입 탐지 및 판단 모듈에서 정상 행위에 대한 서비스 포토별 행위 프로파일과 비교 분석후에 침입 여부를 판단하게 된다.

1) 순차성 탐지 모듈의 순서도

그림2는 순차성을 탐지하기 위한 전체 시스템 모듈의 순서도이다. 이 순서도는 크게 3가지의 모듈로 구성이 되어 있다.

① 감사 자료 수집 모듈

Pcap library는 시스템과 운영체제에 상관없이 패킷 수집이 가능하며, BPF라고 하는 패킷 필터를 사용하여 성능면에서도 우수한 점을 가지고 있는 패킷 수집도구이다. 감사 자료 수집 모듈은 데이터 링크 계층에서 패킷을 수집하는 Pcap library를 이용하여 원시 감사 자료를 수집하게

된다.

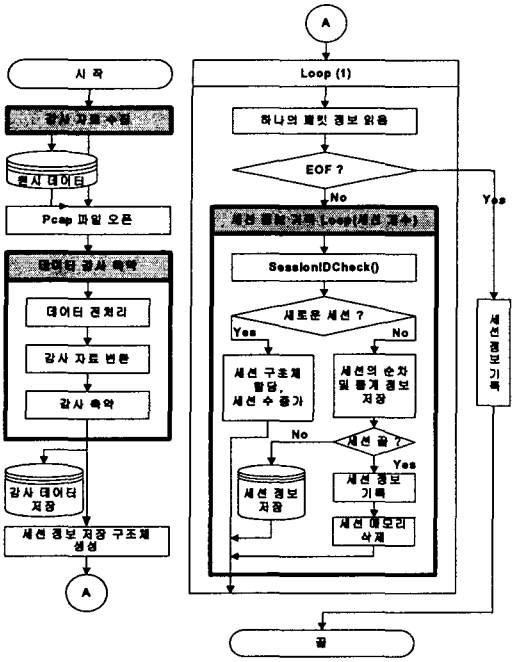

그림 2: 순차성 탐지 모듈의 순서도

② 감사 축약 모듈

침입 탐지에서 사용되는 감사 자료의 사용에 있어 해당 분야의 원시 데이터를 그대로 사용하는 것은 비용측면에서 많은 손실을 발생 할 수 있다. 이러한 이유로 침입탐지시스템에서는 탐지 작업을 하기 전에 일련의 데이터 처리 과정을 거치는데 이 과정에서는 원시 데이터에서 침입탐지에 필요한 요소들만을 추출하여 새로운 데이터(전처리 데이터 : Pre-Processed data)를 형성하게 된다.

본 연구의 전처리 작업에서는 표1과 같이 원시 데이터 내에서 Pcap library 헤더, IP 헤더, TCP 헤더 내의 다음과 같은 요소를 추출하여 새로운 데이터를 형성하게 된다.

③ 세션 정보 기록 모듈

세션 정보 기록 모듈에서는 기록된 감사데이터를 모두 처리하기까지 반복하여 실행된다. 이 모듈에서는 새로운 패킷을 읽을때마다 어느 세션에 속하는지를 파악하고, 새로운 연결을 요청하는 패킷이라면 하나의 구조체 메모리를 할 당해 주고, 그 구조체에 해당 세션에 대한 정보를 저장하게 된다. 만약 해당 세션이 존재하지 않는다면 비정상적인 패킷으로 간주하게 된다.

표 1: 헤더 별 추출 정보

Pcap 라이브러리	timestamp	패킷이 시스템에서 처리되는 시간
IP 헤더	Header Len	IP 헤더의 길이
	Total Len	패킷의 총 길이
	Flag Bit	단편화 bits 정보
	Fragment Offset	단편화 데이터 offset
	Protocol	상위 프로토콜 표현
	Source IP	패킷 송신주 주소
	Dest IP	패킷 목적지 주소
TCP 헤더	Source Port	송신지의 port 번호
	Dest Port	목적지의 port 번호
	Seq Num	패킷의 순차 번호
	Ack Num	패킷의 확인 번호
	TCP 제어 Flag	TCP 패킷의 의미를 표현하는 비트 정보

3. 사용자 행위 테이블

위에서 제안안 시스템에서 네트워크 사용자의 행위를 파악하기 위해 행위 테이블을 생성한다. 이 사용자 행위 테이블은 TCP 연결 설정 단계와 연결 해제 단계에서의 정보를 담아두고 있는데, 그 정보는 순차번호 변이, 확인번호 변이, IP Fragment의 DF 필드 변이, IP Fragment의 MF 필드 변이, IP Fragment Offset의 검사, TCP 제어 플래그의 변이등이 표현된다.

그 밖에도 세션의 활성 시간, 송신지와 목적지의 위치 정보, 유효 패킷 수, 같은 호스트에서 전송되는 Reset의 정기성 검사 등의 기본적인 세션에 대한 정보를 저장하고 있다.

4. TCP 연결 설정 및 연결 해제과정에서의 비정상 행위 탐지

TCP 연결 설정 단계에서는 TCP Flag의 변화 추이, Fragment Offset에 관련한 사항으로 비정상 행위를 측정한다. 그림3의 순서도는 TCP 연결 과정을 나타내고 있다. 일단 처음 패킷을 읽어 오면 그 패킷이 SYN 플래그 인지를 검사하여 새로운 연결에 대한 요청인지를 알아본다. 만약 SYN 플래그가 존재한다면 세션의 정보를 저장을 위한 새로운 메모리를 할당 한다. 만약 SYN 플래그가 존재하지 않는다면, 현재의 패킷이 어떤 세션에 존재하며, 그 세션의 현 상태가 어떤지를 검사하게 된다. 현재 상태가 TCP 연결 설정 단계이면 위와 같은 흐름으로 연결과정에

대한 순차성을 파악하게 된다. 일단 TCP Sequence Number와 Acknowledge Number 정보를 저장하고 새로운 것으로 갱신하며, 패킷의 방향성 및 플래그의 변화 상태를 저장한다. 이렇게 저장된 패킷들은 연결 설정 상태가 종료되었는지 검사를 하여 그정보를 기록하게 된다. 정상 데이터에 대하여 위와 같은 방법으로 기록된 정보는 각 서비스 포트별로 어떻게 상태 변이가 일어났는지를 통계적으로 정리하게 되며, 테스트 데이터로 검증을 할 때 정상데이터에 대한 통계정보를 이용하게 된다.

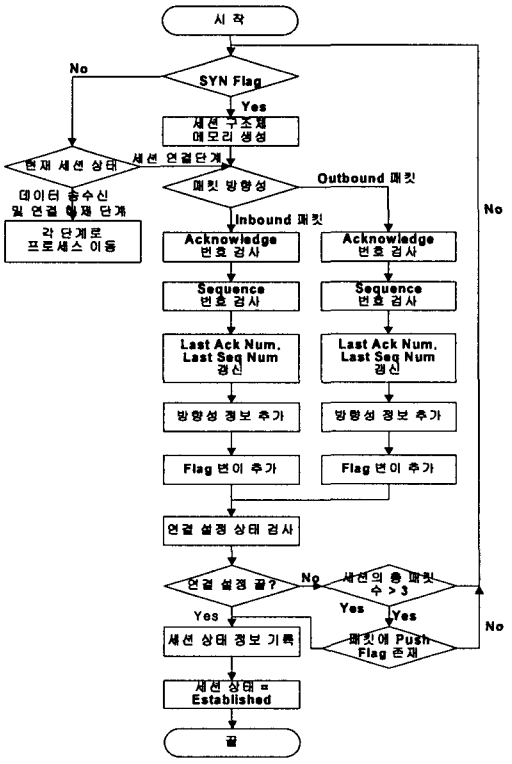

그림 3 TCP 연결 설정 단계에서의 순차성 검증 흐름도

TCP 연결 해제 과정도 위와 같은 순서로 동작을 하게 된다.

IV. 구현 및 결과 분석

1. 시스템 구현 및 실험 환경

본 논문에서 제안한 시스템의 구현환경으로는 Linux Kernel V 2.4.20.8smp의 RedHat 9.1, gcc V3.2.2의 컴파일러 버전, 패킷 수집 도구는 tcpdump 3.7.2를 사용하였다. 네트워크 트래픽을 수집하기 위해 내부 네트워크 주소를 할당하여 그 중 하나를 공격 대상 호스트로 사용하였고, 외부 네트워크에 공격 호스트를 위치시켰다. 모니터링 호스트는 dual-homed gateway로 구성하였다.

2. TCP 연결 설정 단계에서의 실험 결과 및 분석

1) Training Mode

TCP 연결 설정 단계 및 해제단계에 대한 Training Mode의 결과는 Sequence 번호 변이, Acknowledge 번호 변이, IP fragmentation DF 변이, IP Fragmentation MF 변이, IP fragmentation Offset 변이, TCP 제어 플래그 변이의 정보를 표현하며 정상 데이터에 대한 프로파일링 결과를 나타낸다. 이러한 결과는 서비스 포트별 행위 프로파일링 과정을 통하여 클라이언트의 접근 서비스를 기준으로 통계적으로 나타내어진다. 본 논문의 실험은 1999년 DARPA 데이터의 3월 첫 번째 주 월요일 데이터를 사용하였으며 이 데이터는 1369134개의 패킷으로 구성되어 있고, 39811개의 세션이 생성되었으며, 이 데이터에서 사용되는 서비스 포트의 종류는 총 1033개이다. 이 데이터를 Training mode로 처리한 결과는 표 3와 같이 서비스 포트를 중심으로 그 결과가 처리되며, 본 실험에서는 well-known port를 중심으로 한 결과만을 처리 하였다. 이 데이터에서 나타난 well-known port의 종류는 총 11가지(21, 22, 23, 25, 37, 79, 80, 110, 113, 139, 515번)이었으며 각 탐지 메트릭스 별로 그 변이, 빈도수, 확률로 표현되어진다.

2) Test Mode

위와 같이 실험을 통해서 얻어진 정상 행위체 대한 프로파일을 이용하여 침입의 탐지 여부를 알아내기 위하여 1999년 DARPA 데이터의 3월 4째주의 테스트 데이터를 이용하였다.

그 결과 표4와 같은 결과를 얻을 수 있었다. 아래의 표4과 같이 1999년 DARPA 데이터를 이용하여 Training과 Test Mode로 각각 하루치 데이터를 실행 시켜본 결과 총 공격 시도 횟수가 16(UDP제외)회이었고, 그것에 대한 탐지횟수가 9회였다. 즉 탐지율이 약 56%가 도출되었다. 또한 본 논문을 위해 구성했던 실험 환경에서는 네트워크 탐침공격과 서비스 거부공격에 대한 탐지 성능이 뛰어난 것으로 사료된다.

표3: 80번 포토번호에 대한 Training Mode 처리 결과

서비스포트 번호	탐지메트릭	발생 변이(발생 빈도 : 발생 확률)					
80번 (http) 연결 설정 : 35151	Seq 변이	100(35150:100)	00 (1,0)				
	Ack 변이	010(35143:99.98)	000(8:0.02)				
	DF 변이	000(35151:100)					
	MF 변이	000(35151:100)					
	Offset변이	000(2: 0.02)	0064(34367: 97.77)	0640(1: 0.00)	06464(589: 1.68)	64064(84: 0.24)	646464(103 0.29)
	Flag 변이	S>SA<A>(35143:99098)		S>A<R>(7:0.02)		S>R>(1:0)	

표 4: Test Mode의 탐지 결과

공격 이름	탐지 여부	비고
ps		
sendmail		
ntfsdos		
portsweep	O	Reset 패킷의 정기성
sshtrojan Install		
portsweep	O	비정상 패킷(연결설정 무)
xsnoop	O	연결 설정의 플래그 이상
snmpget		
guesstelnet	O	연결 해제의 플래그 이상
portsweep	O	연결 설정에서의 플래그 이상 & Reset 패킷의 정기성
guessftp	O	연결 해제에서의 플래그 이상 & Reset 패킷의 정기성
ftpwrite		
yaga		
crashiis	O	연결 해제의 플래그 이상
portsweep	O	Reset 패킷의 정기성
smurf	O	패킷의 폭주

V. 결론 및 향후 연구

본 논문에서는 일부 비정상행위 침입탐지 방법에서 발생할수 있는 단점인 시간을 기준으로한 트랜잭션(처리 단위)을 사용함으로써 발생 가능한 공격 탐지에 대한 단절 현상을 지적하고 그대안으로 네트워크 세션을 탐지 단위로 사용할 것을 제안한다. 그리고 TCP 연결 설정 과정과 연결 해제 과정에 대한 처리를 실시하여 패킷간의 순차성, 세션간의 순차성과 특정 이벤트의 빈도성 및 정기성 검사를 통하여 네트워크 기반의 공격에 대한 탐지가 가능하다는 것을 알아내었다. 본 연구는 현재 TCP 데이터의 송수신 과정에 대한 프로파일링과 비연결지향성 프로토콜인 UDP/ICMP에 대한 연구도 진행중에 있으며, 앞으로의 연구에서는 좀더 신뢰적이면서 확실한 성능을 밝혀내기 위하여 시스템의 오판율(False Positive / False Negative)을 구할 필요하가 있고, 반복적인 실험을 통하여 절적한 임계치를 설정하는 것이 필요할 것이다. 또한 Training 데이터 및 Test 데이터의 부족으로 인하여 정확한 탐지가 불가능할 수 있기 때문에 신뢰적이면서 더욱 많은 양의 데이터를 이용한 실험도 수반되어야 한다.

참고 문헌

[1] 'MIT Lincoln Laboratory - DARPA Intrusion Detection Evaluation' URL: http://www.ll.mit.edu/IST/indeval/index.html

[2] R. Heady, G. Luger, A. Maccabe, and M. Servilla. "The architecture of a network level intrusion detection system. Technical report", 1990년 8월

[3] http://www.snort.org/cgi-bin/done.cgi

[4] Koral Ilgun "USTAT : A Real-time Intrusion Detection System for UNIX", 1993 IEEE Symposium on Security and Privacy, 1993년 4월

[5] Richard A. Kemmerer "NSTAT : A Model-based Real-time Network Intrusion Detection System", Tech. Report TRCS97-18, University of California, Santa Barbara, 1997년

[6] D. Anderson, T. Frivold, A. Valdes, "Next-generation intrusion detection expert system (NIDES): A summary", Technical Report SRI-CSL-95-07, Computer Science Laboratory, SRI International, Menlo Park, California, 1995년 5월.