韓國 OA學會 論文誌
第5卷 第4號, 2000. 12.

2000-5-4-3-3

삽입 및 배제 공격을 고려한 네트워크 침입 탐지 시스템 모델

차 현 철*

A Network Intrusion Detection System Model for Detecting of Insertion and Evasion Attacks

Hyun-Chul Cha*

요 약

본 논문에서는 삽입 공격과 배제 공격을 탐지할 수 있는 네트워크 침입 탐지 시스템의 모델을 제시하였다. 이를 위해, 먼저 네트워크 침입 탐지 시스템에 대한 공격들을 살펴보았으며, 이들 공격의 탐지에 필요한 정보들을 세 가지 관점에서 분류하였다. 분류된 정보는 탐지를 위한 초기 설정 단계와 실행 단계에서 각각 사용하였다. 제시한 모델은 네트워크 침입 탐지 시스템이 각종 운영체제들의 동작 특성에 대한 정보를 데이터베이스에 유지 및 관리하고 있으며 데이터베이스로부터 테이블을 생성하고, 탐지 시에 이를 참조함으로써 목적지 시스템의 동작을 정확히 예측할 수 있게 된다. 또한, 제시된 모델에서 필요로 하는 데이터베이스와 테이블에 관련된 오버헤더는 별로 크지 않을 것이라 추정할 수 있다.

Abstract

This paper proposes a network intrusion detection model which can detect the insertion and evasion attacks. These attacks can be prevented when some kind of information are available in the network intrusion detection system. We classified these information with three categories and used each category at setup phase and executing phase. Within the proposed model, all necessary information which are related with networks and operating systems are maintained in the database and created as a table. This table is used during intrusion detection. The overheads of database and table may be simple in this model.

* 동양대학교 컴퓨터공학부 조교수

Ⅰ. 서론

침입 탐지(intrusion detection)란 컴퓨터 시스템에 대한 침입을 식별하고 격리시키기 위한 시도를 의미하는 보안(security) 기술을 말하며 보안 시스템의 하나의 중요한 요소로서 다른 보안 기술들을 보완한다. 현재 침입 탐지를 수행하는 다양한 종류의 침입 탐지 시스템들이 존재하며, 침입 탐지 시스템들은 엔진의 타입, 실시간 분석 여부 및 검사하는 데이터의 종류 등에 따라 몇 가지 방법으로 분류 될 수 있다. IDS(Intrusion Detection System)의 엔진은 그 타입에 따라 통계적 비정상 탐지(statistical anomaly detection)와 패턴 매칭 탐지(pattern matching detection) 등으로 분류 할 수 있다. 실시간 실행 여부에 따른 분류에서, 보통 취약점 스캐너(vulnerability scanner)는 주기적으로 실행되는 반면 비정상 탐지기와 패턴 매칭기는 일반적으로 실시간으로 실행된다. 마지막으로 IDS가 검사하는 정보의 종류에 따라 네트워크 데이터와 시스템 데이터 등으로 나누어 볼 수 있다[1-4].

많은 침입 탐지 시스템들은, 단일 컴퓨터 시스템 상에서의 활동(activity)들의 의심스러운 패턴을 감시하기 위해, 운영체제가 제공하는 감사 로그(audit log)를 사용한다. 이런 형태의 IDS들을 호스트 기반(host-based) 침입 탐지 시스템이라 부르며, 로컬 사용자들에 의해 시작되는 단일 시스템의 오 사용(misuses)에 관련된 공격들을 인식하기에 적합하다. 그러나 이 시스템들은 단지 고수준의 로그 정보만을 이용함으로 저 수준에서 발생하는 네트워크 이벤트들에 대해서는 제한된 정보만을 갖게 되는 중요한 단점을 가진다.

네트워크 기반 침입 탐지 시스템(N-IDS:Network-based IDS)들은 네트워크 상에 전송되는 실제 패킷들의 내용을 검사하여 작동한다. 이들 시스템들은 패킷을 분석하고, 네트워크에서 사용되는 프로토콜들을 분석하여 그들로부터 관련되는 정보를 추출해낸다. N-IDS들의 장점을 살펴보면, 먼저, N-IDS는 간단히 구현될 수 있으며 단일 네트워크 상에 존재하는 여러 시스템에 관련된 공격을 식별하는 것 또한 용이하다. 두 번째, N-IDS는 네트워크의 가장 낮은 레벨에서 단순히 청취만 하므로 침입자가 이의 존재를 알기 어렵다. 그러므로 침입자에 의해 시스템이 폐쇄되거나 데이터가 손상되기 어렵다. 세 번째, 스니퍼(sniffer)의 설치로 인한 네트워크의 방해나 네트워크의 성능에 저하가 발생하지 않으므로, 네트워크 상의 다른 시스템들은 스니퍼의 존재에 대해 신경을 쓰지 않아도 된다. 마지막으로, N-IDS가 감시하는 TCP, UDP 등의 네트워크 프로토콜들은 각 시스템에서 사용하는 서로 다른 감사 로그와 달리 표준화되어 있으므로 다른 시스템들과 같이 사용되기 쉽다. 한편, N-IDS는 네트워크 상의 모든 패킷을 볼 수는 없으며, 네트워크 트래픽이 암호화 되어 있을 경우 아무 것도 알 수 없다. 마지막으로, N-IDS가 최종 목적지 노드가 아니라는 단점을 갖는다[3,5].

결국, 호스트 기반 IDS는 네트워크 기반 IDS가 탐지할 수 없는 침입들을 검출 할 수 있으며 반대로 네트워크 기반 IDS는 호스트 기반 IDS가 탐지할 수 없는 침입들을 검출 할 수 도 있다[3]. 그러나 향후 확장일로에 있는 인터넷 등의 발전에 따라 네트워크 기반 공격은 더욱 늘어날 것이며 보다 일반적이고 복잡해 질 것이다. 이러한 이유로 인하여, 침입 탐지 시스템은 침입 활동에 대한 효율적인 탐지 도구를 제공하기 위해, 현재의 호스트 및 운영체제 중심에서 네트워크 자체나 네트워크 IDS로 그 중심을 옮겨 갈 것이다. 이런 종류의 시스템들로는 NSM, DIDS, EMERALD와 NetSTAT 등이 있다[5-7].

현재까지 N-IDS에 대한 많은 연구와 구현이 있어왔다. 현재의 모든 N-IDS는 기본적으로 약점이 많은 수동적 데이터 수집과 프로토콜 분석에 의존하고 있다. 논문[8]에서는 수동적 데이터 수집이 실제 컴퓨터 시스템 상에서 어떤 일들이 일어나고 있는지에 대한 정확한 결론을 얻기에는 통신매체 상에서 얻을 수 있는 정보가 불충분하다는 점을 지적하고 있다. 또한, 네트워크 IDS의 이러한 기본적인 취약점을 대상으로 하는 삽입(insertion) 공격, 배제(evasion) 공격 및 서비스 거부(denial of service) 공격을 정의하고, 현재 가장 많이 사용되고 있는 몇 가지 상용 N-IDS들에 대해 테스트한 결과 이들 모두 이러한 공격에 취약점을 가지고 있음을 보여준다.

네트워크 침입 탐지 시스템은 매우 중요함에도 불구하고 아직도 해결해야할 많은 문제점들을 가지고 있다. 그러므로 본 논문에서는 이상의 점들을 고려하여 N-IDS의 취약점을 보완할 수 있는 방법을 제시하고자 한다.

논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에

서는 네트워크 침입 탐지 시스템에 대한 공격들을 살펴보았으며 3장에서는 삽입과 배제 공격의 탐지에 필요한 각종 정보들을 분류한 후 이를 이용하는 네트워크 침입 탐지 시스템 모델을 제시하였다. 마지막으로 4장에서는 결론과 향후 연구 과제를 다루었다.

Ⅱ. N-IDS에 대한 공격

N-IDS들은 네트워크에 접속된 컴퓨터들이 교환하는 패킷을 청취(sniffering)한 후 프로토콜 분석을 통해 감시하려는 목적지 시스템의 행동을 예측한다. 이러한 방식의 N-IDS들은 기본적으로 두 가지 문제점을 가지고 있다. 첫 번째 문제점은, N-IDS가 전송 매체에서 읽어온 패킷들을 재구성하는 것만으로는 정보가 부족하여 복잡한 프로토콜 트랜잭션 안에서 실제로 어떠한 일들이 일어나는지 정확하게 알기 어렵다는 점이다. 두 번째 문제점으로 N-IDS들은 선천적으로 서비스 거부 공격에 취약하다는 점이다. 본 논문에서는 이 중 첫 번째 문제점에 대해 고려한다.

N-IDS가 사용하는 수동적 네트워크 모니터링 방식은 네트워크 상의 감시하려는 컴퓨터 상에서 실제 어떠한 일들이 발생하고 있는지 정확하게 예측할 수 없다는 단점을 가진다. 일반적으로 N-IDS는 감시하려는 컴퓨터와 완전히 다른 컴퓨터에서 수행되는 경우가 대부분이며, 때로는 완전히 다른 네트워크에 존재하기도 한다. 이러한 상이점으로 인해 N-IDS와 그가 감시하려는 시스템 사이에 불일치가 발생할 수 있다. 이러한 불일치는 기본적인 물리적 차이로 인해 발생하기도 하며 네트워크 드라이브의 구현이 다르기 때문에 기인하기도 한다. 예를 들어, 단일 네트워크의 서로 다른 부분에 위치한 N-IDS와 하나의 종단 시스템을 고려해 볼 때, 이 두 시스템은 서로 다른 위치에서 서로 다른 시간에 임의의 패킷을 수신하게 된다. 이러한 시간적 차이는 중요한 의미를 갖는다. 이 시차 동안에 종단 시스템에서는 어떠한 일이 발생할 수 있으며 이로 인해 패킷의 수신이 되지 않을 수 있다. N-IDS의 특징 인식 시스템이 올바른 정보를 얻지 못하도록 프로토콜 분석을 방해하여 잘못된 결론에 이르게 하는 공격으로는 삽입 공격과 배제 공격이 있다[3,8].

삽입 공격은 공격자가 N-IDS에 잘못된 데이터를 삽입하는 공격을 말한다. 공격자는 N-IDS가 감시하는 종단 시스템은 받아들이지 않지만 N-IDS는 받아들이는 패킷들을 만들어 전송한다. 이 공격을 받는 N-IDS는 종단 시스템이 패킷들을 받아들여 처리하였다고 잘못 판단하지만 실제로 종단 시스템에서는 그러한 일들이 일어나지 않는다. 그림 1은 삽입 공격의 간단한 예를 보여준다. 공격자가 하나의 문자로 된 패킷의 스트림을 전송한다고 가정할 때, 문자 'X'를 갖는 하나의 패킷은 종단 시스템에서는 처리되지 않지만 N-IDS는 받아들이게 된다. 공격자는 이렇게 함으로써 N-IDS에 잘못된 데이터를 삽입할 수 있게 되며 그 결과 종단 시스템에서 보게 되는 문자열과 N-IDS가 보게 되는 문자열은 서로 다르게 된다. 일반적으로 삽입 공격은 N-IDS에서의 패킷 처리가 종단 시스템보다 덜 엄격할 경우에 발생하게 된다.

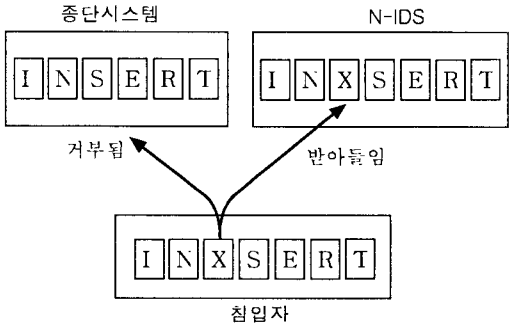

그림 1. 삽입 공격의 예
Fig 1. An example of insertion attack

배제 공격은 삽입 공격과 반대로 종단 시스템은 패킷을 받아들이지만 N-IDS는 패킷의 수신을 거부하는 경우에 발생한다. N-IDS가 실수로 이러한 패킷을 거부할 경우에 전체 내용을 잃어버릴 수 도 있게 된다. 배제 공격은 N-IDS가 지나치게 패킷의 처리에 엄격할 경우에 발생할 수 있다. 배제 공격은 삽입 공격과 마찬가지로 N-IDS와 종단 시스템이 보게되는 문자열이 서로 상이하게 되므로 N-IDS의 패턴 매칭 과정의 실패를 초래할 수 있다. 그림 2는 배제 공격의 예를 보여주고 있다. 이 그림에서 종단 시스템에서는 문자열 "EVASION"을 보게 되나 N-IDS는 문자열 "EASION"만 보게 된다.

일반적으로 삽입공격과 배제 공격은 N-IDS가 임의의 패킷이 종단 시스템에서 받아들여질지 혹은 거부될지를 결정할 수 없는 상황에서 발생한다. N-IDS가 종단 시스템의 행동을

예측할 수 없는 경우는 크게 두 가지의 경우로서 서로 상이한 운영체제와 운영체제의 환경 설정에 기인하는 경우와 네트워크의 토폴로지 및 네트워크의 환경설정에 기인하는 경우로 나누어 볼 수 있다. 먼저, N-IDS가 감시하는 각 종단 시스템은 각기 다른 운영체제를 사용할 수 있으며 서로 다른 각 운영체제는 임의의 패킷에 대해 서로 다른 행동을 취할 수 있다. 기본적인 네트워크 모호성 역시 문제가 될 수 있다. N-IDS가 패킷이 어떤 경로를 따라 목적지에 도달할지 정확히 모르는 경우라면 N-IDS는 패킷이 실제 그곳에 도달할지 알 수 없다. 이런 문제점들을 이용하는 공격들은 N-IDS가 이런 모호성들을 해결할 수 있는 정보를 가지지 않는 한 쉽게 방어될 수 없다. 만약 N-IDS가 종단 시스템에서 실행되는 운영체제를 알 수 있다면 그 시스템에서 채택될지 여부를 판단할 수 있을 것이다. 또한, N-IDS가 네트워크 정보에 대해 신뢰할 만큼 추적할 수 있다면 패킷이 종단 시스템에 의해 받아들여질지 결정할 수 있을 것이다. N-IDS가 임의의 정보를 가진다면 삽입 공격과 배제 공격을 잠재적으로 해결될 수 있으며 이러한 정보에 해당하는 것들로서는 네트워크 위상에 관한 정보, N-IDS가 감시하는 종단 시스템의 환경설정 혹은 운영체제와 버전 정보 등이 있다.

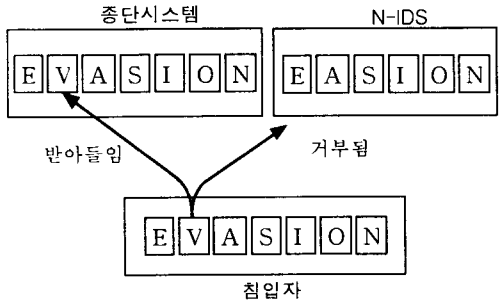

그림 2. 배제 공격의 예
Fig 2. An example of evasion attack

Ⅲ. N-IDS에 대한 침입 탐지 모델

N-IDS에 대한 다양한 삽입 공격과 배제 공격이 존재하므로 N-IDS는 이러한 침입을 탐지할 수 있도록 구축되어야 한다. 본 논문에서는 이들 삽입 및 배제 공격을 탐지할 수 있는 N-IDS의 모델을 제시하고자 한다. 삽입 공격과 배제 공격은 N-IDS가 적절한 정보를 가질 수 있다면 어느 정도 예방될 수 있다. 이들 공격의 예방에 사용될 수 있는 정보들은 대부분 네트워크나 운영체제에 관련된 정보들이며 이들은 그 특성에 따라 몇 가지로 분류해 볼 수 있다. 본 논문에서는 이들 정보들을 그림 3과 같이 세 가지 방법으로 분류하였다.

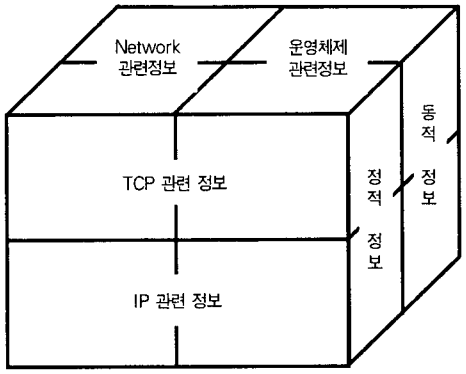

그림 3. 침입 탐지에 사용되는 정보의 분류
Fig 3. Categorizing of the information for intrusion detection

먼저, 침입 탐지에 사용되는 정보들은 정보가 얻어지는 근원에 따라 네트워크에 관련된 정보와 운영체제에 관련된 정보로 구분해 볼 수 있다. 네트워크에 관련된 정보들로는 N-IDS와 N-IDS가 보호하려는 목적지 시스템이 속한 각 네트워크 토폴로지, 네트워크의 환경 설정, 및 각 네트워크간의 관계 등에 관련된 정보들이 있으며 이들은 N-IDS가 자체적으로 수집할 수 있는 특성을 갖는다. 운영체제에 관련된 정보들로는 목적지 시스템들에서 사용되는 운영체제의 종류와 버전, 운영체제의 환경 설정 등이 있으며, 이러한 정보들은 목적지 시스템의 협조 없이는 수집하기 어렵다는 특징을 갖는다. 두 번째로 사용자 정보가 인터넷 등에서처럼 TCP/IP 프로토콜을 사용하여 통신된다고 가정하면, 사용자 정보는 TCP와 IP의 헤더가 덧붙여져 전송되며 N-IDS는 네트워크에서 청취한 패킷에 대해 헤더 정보를 각 프로토콜 단계별로 분석하게 된다. 그러므로 프로토콜 분석 단계별로 분류해 보면, IP 혹은 그 하위 계층(예를 들어, MAC 계층)의 헤더 분석 시 필요한 정보와 TCP 혹은 그 상위 계층 헤더를 분석할 때 사용하는 정보로 분류할 수 있다. 마지막으로, 획득된 정보가 얼마나 자주 변경되는가에 따라, 정적 정보

와 동적 정보로 구분할 수 있다. 네트워크의 토폴로지 및 환경 설정, 운영체제의 종류 및 환경 설정 등 대부분의 정보들은 한번 결정되면 쉽게 변하지 않는 정적 혹은 준-정적 특성을 가지나 TCP 윈도우의 크기, 목적지 시스템에서 프레그먼트 큐의 상태 등의 정보들은 통신 중에 수시로 변하는 동적인 특성을 갖는다.

본 논문에서는 삽입 공격과 배제 공격의 탐지에 필요한 각종 정보들을 일단 정적 정보와 동적 정보로 구분하였다. 동적 정보의 수집 및 이에 기초한 침입의 탐지는 N-IDS에 상당한 부담을 가져오며 [9]에서처럼 특별한 방법이 고려되어야 하므로 본 논문에서는 고려하지 않는다. 다음, 이들 정적 정보들을 네트워크 정보와 운영체제 정보로 구분하였다. 네트워크 관련 정보들은 N-IDS에서 자체적으로 수집할 수 있으나 운영체제 관련 정보들은 감시하려는 목적지 시스템으로부터 최소한 운영체제의 종류와 버전 정보 정도는 제공받아야만 올바른 정보를 수집할 수 있게 되므로, 이들 분류는 N-IDS에서의 정보 수집의 방향을 결정하는데 사용하였다. 마지막으로 정보들은 프로토콜에 따른 분류를 하여 IP (혹은 그 하위 계층) 관련 정보와 TCP 관련 정보로 구분하였으며 UDP 혹은 TCP 상위 계층들은 고려하지 않았다. 이 분류는 N-IDS가 네트워크 상의 임의의 패킷을 청취한 후 헤더에 부착된 정보를 바탕으로 프로토콜 분석을 단계적으로 실행하게 되므로 각 프로토콜 분석 단계에서 필요한 정보들을 참조하기 위함이다.

삽입 공격과 배제 공격을 탐지하기 위한 침입 탐지 시스템의 구성은 그림 4와 같다.

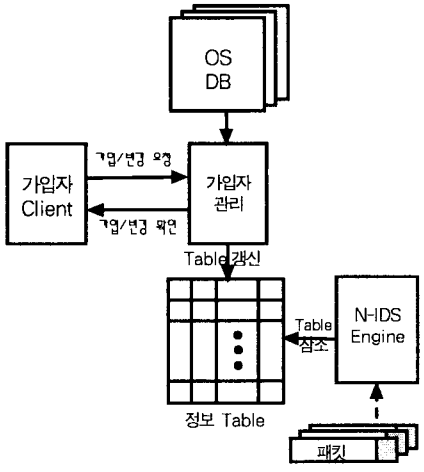

그림 4. 침입 탐지 시스템의 구성
Fig. 4. Configuration model of the proposed intrusion detection system

먼저 가입자 클라이언트 모듈은 목적지 시스템에서 실행되며 N-IDS의 보호를 원할 경우 N-IDS로 가입 신청을 하거나 정적 정보가 변하게 되면 변경 요청을 하게 된다. N-IDS의 가입자 관리 모듈은 가입자 클라이언트로부터의 요청을 처리하고 확인해 주며 가입자에 관련된 정보를 수집하고 정보 테이블을 생성 및 갱신하는 역할을 담당한다. 가입자 관리 모듈은 가입자 클라이언트로부터 가입 요청이 오면 먼저 가입자의 네트워크에 관련된 각종 정보들, 예를 들어 가입자 네트워크의 최대 세그먼트 크기, 가입자까지의 홉 수 등과 같은 네트워크 정보들을 수집한 다음 가입자에게 운영체제 정보를 요청하게 된다. 가입자는 N-IDS로부터 보호받기 위해서는 자신의 운영체제 종류 및 환경설정에 관한 내용을 N-IDS에 알려주어야 한다. 가입자 관리 모듈은 자체적으로 미리 유지하고 있는 OS 데이터베이스에서 해당 운영체제에 관한 내용을 읽어와, 수집한 네트워크 관련 정보와 더불어 정보 테이블에 항목을 기록하게 된다. 아울러, 가입자 관리 모듈은 이미 정보 테이블이 생성되어 있더라도 주기적으로 네트워크 관련 정보를 수집하여 네트워크 정보의 변경에 대처하여야 한다. 실행 시, N-IDS 엔진은 네트워크로부터 패킷을 청취하였을 때, 정보 테이블을 참조하여 삽입 공격과 배제 공격에 대처할 수 있게 된다.

한편, 정보 테이블의 각 항목, 즉, 테이블에서 유지되어야 하는 정보는 그림 5와 같이 크게 IP 관련 정보와 TCP 관련 정보로 분류하였다. IP 관련 정보에는 MAC 주소, IP 주소 및 각 운영체제마다 다른 각종 IP 옵션 처리 방법들이 있으며, TCP 관련 정보에는 목적지 시스템의 포트에 관련된 정보들과 서로 다른 TCP 옵션 처리 방법에 관한 정보들을 유지하게 된다.

IP 관련 정보				TCP 관련 정보		
MAC 주소	IP 주소	각종 IP 옵션 처리 방법	. . .	port 정보	각종 TCP 옵션 처리 방법	. . .

그림 5. 침입 탐지 시스템의 테이블 항목
Fig. 5. A table entry of IDS

그림 5에서 분류한 각 정보들의 상세한 정보 종류 및 이들 정보의 사용 용도를 표 1과 표 2에서 보였다. 이 표에서 발생가능 문제점은 삽입 공격과 배제 공격이 발생할 수 있는 가능성을 설명하고 있으며 이런 문제점을 해결하기 위해 각 정보들이 사용되게 된다. 표 1은 IP 관련 정

보에 대한 설명이며 표 2는 TCP 관련 정보에 대해 설명하고 있다. 표 1과 2에 나타나는 TCP/IP의 구체적 동작 방법과 발생 가능 문제점은 [10]과 [8]에서 각각 구체적으로 설명하고 있다.

표 1. IP 관련 정보 종류
Table. 1 Information which related with IP

정보 종류	발생 가능 문제점
MAC 주소	목적지의 MAC 주소가 틀리면 목적지에서 폐기 (IP 주소는 올바름)
hop 수	TTL 값에 따라 N-IDS는 받아들이나 목적지 네트워크에서는 볼 수 없음
최대 단편 크기	N-IDS와 목적지 시스템이 속한 네트워크의 최대 단편 크기가 다른 경우 공격 가능 (DF bit 설정된 경우)
source-routed IP 옵션 거부 여부	목적지가 source-routed 패킷을 폐기할 수 있음
timestamp IP 옵션 처리 방법	목적지가 부분적으로 수신한 단편들을 서로 다르게 timeout 할 수 있음
중첩된 단편 처리 방법	중첩된 단편 처리 방법이 OS 마다 다름
단편에 나타나는 IP 옵션 처리 방법	단편에 나타나는 IP옵션 처리 방법이 OS 마다 다름

표 2. TCP 관련 정보
Table. 2 Information which related with TCP

정보 종류	발생 가능 문제점
Code 필드의 비정상 flag 처리 방법	OS에 따라 비정상적 flag 가진 패킷 폐기하지 않는 경우 있음
ACK flag 설정 안된 패킷 처리 방법	목적지가 특정 옵션 실어 나르는 TCP 패킷 채택하지 않을 수 있음
SYN 패킷에 포함된 data 처리 방법	목적지가 특정 옵션 실어 나르는 TCP 패킷 채택하지 않을 수 있음
틀린 체크섬을 가진 패킷 처리 방법	OS가 틀린 체크섬을 검사하지 않을 수 있음
non SYN 단편이 TCP 옵션을 가졌을 때 처리 방법	목적지가 특정 옵션을 실어 나르는 TCP 패킷을 채택하지 않을 수 있음
TCP 단편의 중첩 처리 방법	OS마다 중첩된 단편 처리 방법이 다름
RST 패킷의 일련번호 검사 여부	목적지가 RST패킷의 일련 번호를 검사하지 않는 경우 있음

본 논문에서 제시한 삽입 및 배제 공격을 탐지하기 위한 N-IDS 모델에서는 먼저, N-IDS가 네트워크에서 사용되는 각종 운영체제들의 동작 특성에 대한 정보를 데이터베이스에 유지 및 관리하고 있어야 한다. 보호를 원하는 목적지 시스템은 자신의 운영체제의 종류에 대한 정보를 N-IDS에 제공해 주어야 하며, N-IDS는 가입 요청을 받은 시점에서 수집한 네트워크 관련 정보들과 데이터베이스에서 추출한 운영체제 관련 정보들을 합쳐 테이블의 항목을 생성한다. 이 때, 테이블의 항목은 프로토콜 분석 단계별로 정렬되게 된다. N-IDS 엔진은 네트워크에서 패킷을 캡쳐 하여 삽입 및 배제 공격에 대한 탐지가 필요할 경우 테이블을 참조하여 목적지 시스템의 동작을 정확히 예측할 수 있게 된다.

이러한 시스템을 구축하기 위해 필요로 하는 데이터베이스와 테이블에 대해 알아보면, 먼저, N-IDS가 유지해야하는 OS 데이터베이스의 크기는 현재 시중에서 사용중인 운영체제의 종류가 그리 많지 않음에 비추어 별로 크지 않아도 될 것이다. 고속 메모리에서 관리되어야 하는 테이블의 항목 수는 N-IDS가 감시하는 목적지 시스템의 수에 비례하게 되며 현실적으로 하나의 N-IDS가 감시할 수 있는 목적지 시스템의 수가 제한되므로 테이블의 크기는 아주 작게 유지될 수 있을 것이다. 그러므로, 침입 탐지 시스템에서 삽입 공격과 배제 공격을 탐지하기 위해 추가되어야 하는 오버헤더는 별로 크지 않을 것이다.

Ⅳ. 결 론

침입 탐지 시스템의 중요성은 인터넷 등의 발전과 더불어 날로 그 중요성을 더해가고 있다. 본 논문에서는 침입 탐지 시스템을 살펴보고 특히, 네트워크 침입 탐지 시스템에 초점을 맞추어 그 취약점을 고찰하였다. N-IDS는 아직 해결되지 않은 몇 가지 약점을 가지고 있으며 본 논문에서는 그 중에서 특히, 삽입 공격과 배제 공격을 탐지할 수 있는 시스템 모델을 제시하였다.

이를 위해, 먼저, 삽입 및 배제 공격의 예방에 사용될 수 있는 정보들을 그 특성에 따라 정적 정보와 동적 정보, 네트워크 관련 정보와 운영체제 관련 정보, TCP 관련 정보와 IP 관련 정보 등의 세 가지 방법으로 분류하였다.

본 논문에서 제시한 삽입 및 배제 공격을 탐지하기 위한 N-IDS 모델에서는 먼저, N-IDS가 네트워크에서 사용되는 각종 운영체제들의 동작 특성에 대한 정보를 데이

터베이스에 유지 및 관리하고 있게 된다. N-IDS로부터 보호를 원하는 목적지 시스템은 자신의 운영체제의 종류에 대한 정보를 N-IDS에 제공해 주어야 하며, N-IDS는 가입 요청을 받은 시점에서 수집한 네트워크 관련 정보들과 데이터베이스에서 추출한 운영체제 관련 정보들을 합쳐 정보 테이블의 항목을 생성한다. N-IDS 엔진은 네트워크에서 패킷을 캡처 하여 삽입 및 배제 공격에 대한 탐지가 필요할 경우 테이블을 참조하여 목적지 시스템의 동작을 정확히 예측할 수 있게 된다.

N-IDS가 유지해야하는 데이터베이스의 크기는 현재 사용중인 운영체제의 종류가 그리 많지 않음에 비추어 별로 크지 않아도 될 것이다. 메모리에서 관리되어야 하는 테이블의 항목 수는 N-IDS가 감시하는 목적지 시스템의 수에 비례하며 현실적으로 하나의 N-IDS가 감시할 수 있는 목적지 시스템의 수가 제한되어 있으므로 테이블의 크기는 아주 작게 유지될 수 있을 것이다. 결국, 침입 탐지 시스템에서 삽입 공격과 배제 공격을 탐지하기 위해 추가되어야 하는 오버헤더는 별로 크지 않을 것이다.

본 논문의 향후 연구과제는 N-IDS에서 네트워크와 운영체제에 관련된 정보들을 효율적으로 수집 및 관리하는 방법과 실제 네트워크 환경에서 이를 구현하는데 필요한 추가적인 연구가 수행될 것이다.

참고 문헌

[1] D. E. Denning, "An Intrusion-Detection Model," Proc. of the IEEE Symposium on Security and Privacy, pp. 118-131, 1986.

[2] 한국정보보호센터, 실시간 네트워크 침입 탐지 시스템 개발에 대한 연구, Dec., 1998.

[3] T. Escamilla, Intrusion Detection Network Security Beyond the Firewall, Addison-Wesley, 1998

[4] S. Kumar, E. Spafford, "A pattern matching model for misuse intrusion detection," Proc. of the 17th National Computer Security Conference, pp. 11-21, Oct., 1994.

[5] A. Sundaram, "An Introduction to Intrusion Detection, "http://www.acm.org/crossroads/xrds2 -4/intrus.html

[6] G. Vigna, R. A. Kemmerer, "NetSTAT : A Network-based Intrusion Detection Approach," Proc. of ACSAC'98, 1998.

[7] 김병구, 정태명, "침입탐지 기술의 현황과 전망," 정보과학회지, 18권 1호, pp.29-39, Jan., 2000.

[8] T. H. Ptacek, T. N. Newsham, "Insertion, Evasion and Denial of Service : Eluding Network Intrusion Detection,"http://www nai.com/products /security/advisory/papers/ids.pdf, Jan., 1998.

[9] 차현철, "네트워크 침입 탐지 시스템에서의 시차 문제 해결 방안," 한국산업정보학회 논문지, 심사중, Sep., 2000.

[10] W. R. Stevens, TCP/IP illustrated, Vol. 1, Addison-Wesley, 1994.

저자소개

차 현 철

1988 경북대학교 통계학과(학사)

1993 경북대학교 컴퓨터공학과 (석사)

1998 경북대학교 컴퓨터공학과 (박사)

2000 Arizona State Univ. (Post-Doc.)

1995-현재 동양대학교 컴퓨터 공학부 조교수

관심분야 : B-ISDN/ATM, Wireless ATM, 광 인터넷, 네트워크 보안, 침입 탐지