웹기반의 침입탐지 트래픽 분석 시스템 설계

Design of Web based ID Traffic Analysis System

한순재, 오창석
충북대학교

Han Soon-Jae, Oh Chang-Suk
Chungbuk National Univ.

요약

기존의 Snort와 같은 침입탐지시스템은 수없이 많은 경고 메시지를 관리자의 화면상에 표시함으로써 해당 관리자를 혼란에 빠트려 해킹 초기 대응능력을 무력하게 만드는 문제점과 함께 false positive 오류 가능성을 내포하고 있다. 이에 본 논문에서는 이러한 문제점들을 해결하기 위해 상관성을 이용한 웹 기반의 침입 탐지 트래픽 분석 시스템을 설계하였으며 Libpcap, Snort, ACID, Nmap, Nessus를 도구로 사용, 트래픽을 일반 트래픽과 침입 트래픽으로 구분하여 관리자가 전체 침입 탐지 트래픽 상황을 웹 상에서 쉽게 확인할 수 있도록 구현하였다. 그 결과 경고메시지 및 false positive 오류를 최소화시킬 수 있었다.

Abstract

A general administrator's response ability plunged in confusion as intrusion detection system like an existing Snort display much alert messages on administrator's screen. Also, there are some possibilities to cause false positive. In this paper, to solve these problems, we designed Web-based ID(Intrusion Detection) traffic analysis system using correlation, and implemented so that administrator can check easily whole intrusion traffic state in web which dividing into normal and intrusion traffic using Libpcap, Snort, ACID, Nmap and Nessus. As a simulation result, it is proved that alert message number and false positive rate are minimized.

I. 서론

국가·사회의 기반 구조가 점차 정보 통신 인프라에 절대적으로 의존하고 있으며 사이버 공간은 이미 제2의 생활공간으로 자리잡고 있다. 그러나 정보의 증가와 더불어 해킹·바이러스의 지능화, 불건전 정보 유통의 증가, 사생활 침해 등 정보화 역기능이 두드러지게 나타나고 있으며 이에 대한 사회적 혼란이 가속화되고 있다[1]. 그러나 인터넷보안관련회사 및 대기업을 제외하고는 보안전문가가 아닌 일반 전산직 관리자가 기업 내의 시스템 및 네트워크를 관리하고 있다. 따라서 외부의 공격이 있을 경우 기존의 Snort와 같은 침입탐지시스템은 그 기능이 막강한 반면 너무 많은 경고메시지를 화면상에 표시, 해킹 초기 대응 능력을 무력하게 만들고 침입탐지 트래픽이 전체 트래픽 중 어느 정도를 차지하고 있는지, 각 IP별 침입탐지 트래픽 발생량이 어느 정도인지를 효과적으로 제시하지 못하고 있는 실정이다.

본 논문에서는 이러한 문제점들을 해결하기 위해 기존 경고메시지의 필터링 및 상관성을 이용한 웹기반의 침입탐지트래픽 분석시스템을 설계하고 Libpcap, Snort, ACID, Nmap, Nessus를 이용하여 전체 트래픽을 일반 트래픽과 침입 트래픽으로 구분, 각각의 트래픽을 프로토콜별, 서비스별, IP별로 표시하여 관리자가 전체 침입 탐지 트래픽 상황을 웹 상에서 쉽게 확인할 수 있도록 하고 경고메시지 및 false positive가 최소화된 효율적인 웹 기반의 침입 탐지 트래픽 분석 시스템을 구현하고자 하였다.

II. 경고메시지의 상관성 분석

2.1 유사성에 기초한 확률적인 방법

전체 유사성은 특징 유사성들의 가중 평균으로 구하며 새로운 경고메시지가 기존의 메타 경고메시지와 비슷할 경우 같은 그룹으로 묶여지며 그렇지 않을 경우 새로운 경고메시지는 새로운 메타 경고메시지 쓰레드를 생성하여 다음 경고메시지와 비교된다[2]. 이 기법은 경고메시지 사이의 인과 관계를 발견하기가 곤란하며 유사성이 낮은 공격을 탐지하기 어렵다는 문제점을 가지고 있다.

세부적인 기법은 식 1과 같이 기존 메타 경고메시지와 새로운 침입 경고메시지간의 유사가능성을 구해 상관성 분석을 한다.

$$SIM(X,Y) = \frac{\sum_j E_j SIM(X_j, Y_j)}{\sum_j E_j} \qquad (1)$$

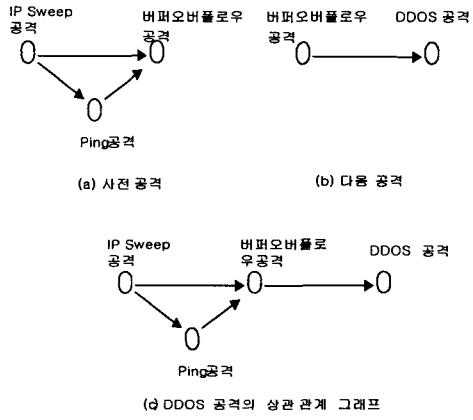
여기서 SIM(X,Y)는 X와 Y의 유사성, X는 메타 경고메시지, Y는 새로운 경고메시지, j는 특징 경고메시지의 인덱스, E_j는 특징 j의 유사성의 평균, X_j와Y_j는 X,Y의 특징 j의 값이다.

2.2 정의된 공격 상태 그룹에 의한 ACC 방법

ACC(Aggregation and correlation component)는 여러 침입탐지시스템인 프로브로부터 경고메시지를 획득한 후 중복, 연속된 것은 동일한 공격 유형 상관관계(correlation relationship)로 판단하고 출발지주소, 목적지주소, 공격의 유형에 따라 7가지 상태 그룹관계(aggregation relationship)로 판단하여 관리자에게 농축된 경고메시지 결과를 제공한다. 경고메시지 클래스 계층은 프로브가 탐지한 경고메시지의 기본 정보를 담고 있는 probe 계층, 목적지주소 정보를 담고 있는 target 계층, 출발지주소 정보를 담고 있는 source 계층, 세부적인 서비스의 정보를 담고 있는 detailed target 계층으로 구분된다[3]. 이 기법은 미리 정의된 공격 상태 그룹에 해당하지 않는 공격이 있을 경우 문제점이 발생한다.

2.3. 공격의 전제조건을 이용한 유사성 평가 방법

공격의 전제조건을 이용하여 경고메시지의 유사성을 평가하는 방법으로 특정 사전 공격은 사후 공격을 위한 준비 단계라는 것을 이용한다[4]. 그림 1과 같이 공격의 절차를 밝혀 낼 수 있고 공격이 시도되었을 경우 공격의 진행을 예상할 수 있는 장점이 있으나 특정 공격을 탐지하지 못하거나 공격이 사후 공격의 정보를 충분히 제공하지 않을 경우 상관관계 분석을 하지 못한다는 단점이 있다.



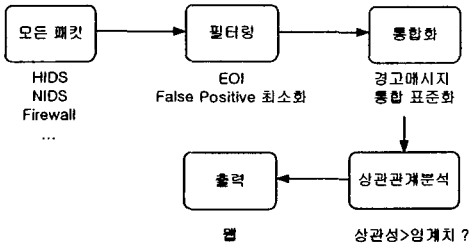
▶▶그림 1. 공격의 전제조건을 이용한 상관관계 그래프

III. 상관성을 이용한 침입탐지 트래픽 분석

본 논문에서 제시하는 상관성을 이용한 웹 기반의 침입탐지 트래픽 분석 시스템의 설계 목표와 시스템 구성은 다음과 같다.

3.1 설계 목표

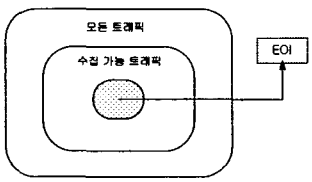
본 논문에서 제안하고자 하는 상관성을 이용한 웹 기반의 침입탐지 트래픽 분석 시스템의 설계 목표는 그림 2와 같이 크게 4가지로 구분할 수 있다.



▶▶ 그림 2. 시스템 설계

(1) 필터링을 통한 최소한의 false positive EOI 선택

네트워크의 속도가 점차 고속화됨으로 인해 모든 트래픽의 침입탐지 여부 판별 자체는 불가능하다. 그리고 침입탐지시스템의 false positive 및 false negative로 인한 탐지 오류가 발생할 가능성이 매우 크다. 따라서 본 논문에서 제시하는 시스템에서는 그림 3과 같은 관심 사건 대상인 EOI(Events of Interest)[5]의 필터링을 통하여 false positive가 최소화 된 침입 탐지 트래픽을 분석한다.



▶▶ 그림 3. EOI

(2) 경고메시지의 통합화

필터링을 통한 EOI 침입탐지 경고메시지들은 침입탐지시스템에 따라 형태가 다르게 나타난다. 이러한 경고메시지를 모든 침입탐지시스템이 공유할 수 있도록 통합 표준화한다.

(3) 상관성 분석을 통한 침입 판단

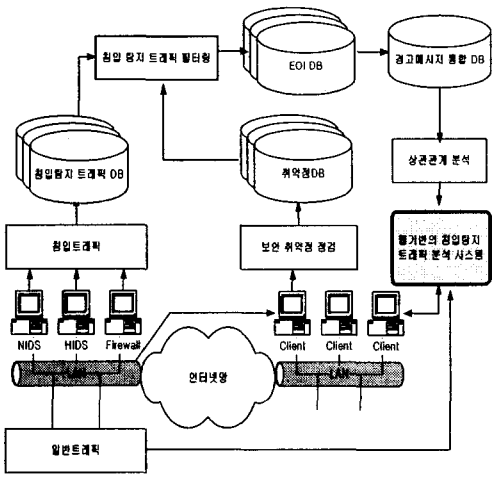
여러 침입 탐지 트래픽의 상관 관계를 분석한 후 특정 임계치를 초과할 경우 최종적으로 침입 트래픽으로 판단한다.

(4) 사용자 관점의 침입 탐지 트래픽 출력

최종적으로 침입으로 판단된 트래픽을 웹 상에서 쉽게 확인할 수 있도록 하되 보안 전문가가 아닌 일반 네트워크 관리자 측면에서 쉽게 이해할 수 있고 일반 사용자들에게 보안의 중요성에 대해 객관적으로 설명할 수 있는 근거 자료가 되도록 보안 대상 호스트 프로토콜별, 서비스별, IP별로 침입탐지 트래픽 비율을 화면상에 출력한다.

3.2 시스템 구성

본 논문에서 제시하고자 하는 시스템의 구성은 그림 4와 같다. 네트워크 상의 패킷이나 보안 관련 각종 로그를 NIDS, HIDS, firewall등 여러 보안 관련 시스템이 침입 트래픽을 자체적인 시그너처 및 규칙집합에 의거 탐지하고 침입 탐지 트래픽 데이터베이스에 저장한다. 그 후 보안 취약점 데이터베이스와 비교, 불필요한 패킷 및 이벤트들을 필터링한다. 필터링 된 결과는 false positive가 최소화 된 EOI 데이터베이스에 삽입되고 다시 통합된다.



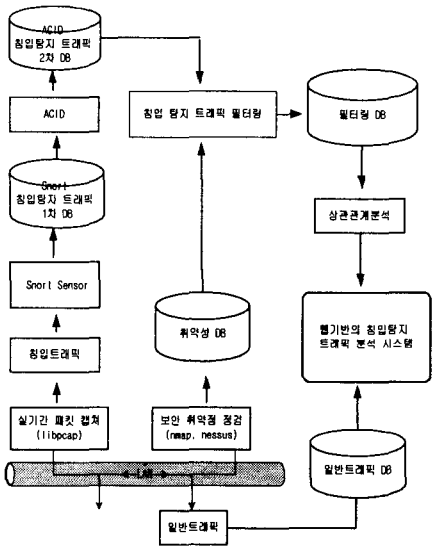
▶▶ 그림 4. 시스템의 구성도

마지막으로 상관분석을 통해 최종적으로 침입 트래픽 판단을 내리고 그 결과를 웹 상에서 보여준다.

3.3 시스템 구현

본 논문에서 구현한 시스템은 그림 5와 같이 우선 침입 트래픽과 일반 트래픽을 따로 데이터베이스에 저장한다. Libpcap을 이용하여 LAN상의 모든 패킷을 실시

간으로 캡처한 후 침입 트래픽일 경우 NIDS인



▶▶ 그림 5. 시스템 구현도

Snort가 자동으로 감지하여 침입 탐지 트래픽 1차 데이터베이스에 저장하고 일반 트래픽일 경우 감시 하고자 하는 호스트에 해당하는 정보만을 일반 트래픽 데이터베이스에 저장한다. 침입 트래픽으로 판단되어 MySQL 데이터베이스에 저장된 Snort의 각종 경고메시지들은 ACID을 거쳐 침입 탐지 트래픽 2차 MySQL 데이터베이스에 저장된다. 이렇게 저장된 2차 침입 탐지 트래픽 데이터베이스의 자료들은 Snort의 각종 경고메시지들로 웹 상에서 바로 보여주기에는 너무 많은 경고메시지를 가지고 있어 오히려 네트워크 관리자에게는 매우 혼란스러운 형태로 나타난다.

따라서 본 논문에서는 ACID가 생성한 침입 탐지 트래픽 2차 데이터베이스 중 불필요한 경고메시지나 false positive의 가능성이 있는 경고메시지를 제거한다. 그 방법으로는 우선 감시하고자 하는 호스트들을 Nmap과 Nessus을 이용하여 보안 취약점 점검을 한다. 그 후 보안 취약점 점검으로 인해 생성된 취약점 데이터베이스와 2차 침입 탐지 트래픽 데이터베이스를 비교하여 불필요한 데이터를 필터링 한다. 마지막으로 생성된 필터링 데이터베이스의 자료 중 동일한 목적지주소, 포트번호, 공격유형별로 그룹화하고 식 2에 따라 상관분석 작업을 진행한 후 지정한 임계치를 초과할 경우 침입 트래픽으로 최종 판단을 내리고 웹 상에서 일반 트래픽과 침입 트래픽으로 구분하여 프로토콜별, 서비스별, IP별로 네트워크 관리자에게 보여준다.

$$C(i,j,k)=i+Min(j,k)>=1.25 \qquad (2)$$

단, i는 운영체제의 적합성,
j는 시그너쳐의 위험도,
k는 Nessus의 취약점
$C(i,j,k)$는 비교항목간의 상관성 판단 기준,
$Min(j,k)$는 j와 k의 최소값

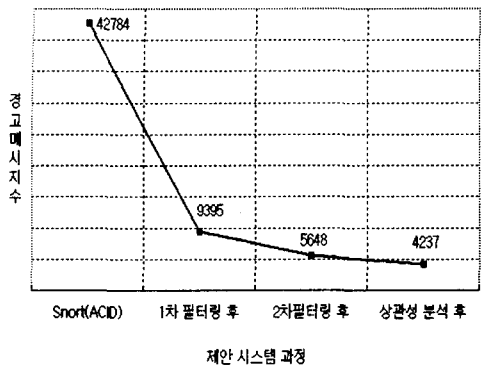
Ⅳ. 실험 및 결과 고찰

본 논문에서 제안한 상관성을 이용한 웹 기반의 침입 탐지 트래픽 분석 시스템에 대한 false positive 오류율을 Snort(ACID)와 비교한 결과 표 1과 같이 제안 모델이 19.23%정도 우수함을 알 수 있었다.

[표 1] 제안 모델의 성능비교

비교 항목	탐지 패킷	정상 패킷	침입 패킷	False Positive
Snort(ACID)	4404개	2840개	2564개	64.49.%
제안시스템	1739개	787개	952개	45.26%

또한 제안 모델의 필터링 및 상관 관계 분석 과정별 경고메시지의 변화 결과를 2003년 10월 5일부터 10월 14일 기간 동안 수집된 패킷을 기준으로 살펴본 결과 그림 6과 같이 90.1%의 경고메시지 감소 효과를 볼 수 있었다.



▶▶ 그림 6. 과정별 경고메시지 변화

V. 결론

본 논문에서는 경고메시지 및 false positive rate 감소를 위해 Libpcap, Snort, ACID, Nmap, Nessus를 도구로 사용, 상관성을 이용한 웹 기반의 침입 탐지 트래픽 분석 시스템을 설계하였으며 트래픽을 일반 트래픽과 침입 트래픽으로 분류하고 각각의 트래픽을 프로토콜별, 서비스별, IP별로 구분하여 관리자가 전체 침입 탐지 트래픽 상황을 웹 상에서 쉽게 확인할 수 있도록 구현하였다. 구현된 상관성을 이용한 웹 기반의 침입 탐지 트래픽 분석 시스템의 성능 분석 결과 경고메시지 및 false positive를 줄일 수 있었으며 크래커에 의한 외부 공격이 발생할 경우 관리자의 초기 대응 능력 향상을 기대할 수 있었다. 특히 침입 트래픽이 많이 발생한 IP 사용자에게 보안의 필요성을 확연히 설명해 줄 수 있는 계기를 마련하였다.

본 연구에 대한 향후 연구 과제로는 설계 목표에서 제시한 경고메시지의 통합에 대한 연구이다. 또한 제한 모델의 부족한 부분인 침입 탐지 트래픽의 히스토리 기능 및 검색 기능을 강화하는 방법에 대한 연구가 필요하다.

▮참고문헌▮

[1] 오창석, 데이터 통신, 영한 출판사, 2001
[2] A. Valdes and K. Skinner, "Probabilistic alert correlation", RAID 2001, pages 54-68, 2001.
[3] H. Debar and A.Wespi, "Aggregation and correlation of intrusion-detection alerts" , In Recent Advances in Intrusion Detection, 2001.
[4] P. Ning and Y. Cui, "An intrusion alert correlator based on prerequisites of intrusions" , North Carolina State University, January 2002.
[5] Stephen Northcutt, Judy Novak, 네트워크 침입탐지와 해킹 분석 핸드북, 인포북, 2001.