韓國컴퓨터情報學會 論文誌
第14卷 第5號, 2009. 5.

2009-14-5-3-1

False Alarm 감축을 위한 효율적인 공격 트래픽 탐지 기법

최 일 준**, 추 병 균*, 오 창 석**

Efficient Attack Traffic Detection Method for Reducing False Alarms

Il-Jun Choi **, Byoung-Gyun Chu *, Chang-Suk Oh **

요 약

IT의 발전으로 많은 컴퓨터 사용자들이 인터넷 사용을 생활화하고 있다. HTML 기술을 이용한 웹 기술의 발전은 현대인들의 정보를 빠르고 쉽게 공유할 수 있도록 하고 있으며, 그 이용이 기하급수적으로 증가하고 있는 추세이다. 그러나 그에 따른 부작용으로 중요 시스템에 대한 정보 유출, 전산망 침해 등과 같은 침입 행위 또한 빠른 속도로 증가하고 있다. 이에 본 논문에서 제안하는 공격 트래픽 탐지 기법은 전통적인 네트워크기반 공개 침입탐지시스템인 Snort를 이용하여 탐지한 공격 트래픽 중 false positive 가능성이 있는 패킷을 Nmap 정보를 이용하여 필터링 하고, nessus 취약점 정보를 이용하여 2차 필터링을 실시한 후, 운영체제의 적합성, 시그너처 위험도, 보안 취약점을 고려하여 상관성 분석을 최종적으로 실시하여 false positive 경고 메시지를 줄이고 false positive에 의한 오류를 최소화하여 전체적인 공격 탐지 결과를 높였다.

Abstract

The development of IT technology, Internet popularity is increasing geometrically. However, as its side effect, the intrusion behaviors such as information leakage for key system and infringement of computation network etc are also increasing fast. The attack traffic detection method which is suggested in this study utilizes the Snort, traditional NIDS, filters the packet with false positive among the detected attack traffics using Nmap information. Then, it performs the secondary filtering using nessus vulnerability information and finally performs correlation analysis considering appropriateness of management system, severity of signature and security hole so that it could reduce false positive alarm message as well as minimize the errors from false positive and as a result, it raised the overall attack detection results

▸ Keyword : 트래픽 탐지(Traffic Detection), 분산 서비스거부공격(DDos), NIDS(Network-IDS), Snort

• 제1저자 : 최일준 교신저자 : 오창석(csoh@chungbuk.ac.kr)
• 투고일 : 2009. 01. 21, 심사일 : 2009. 04. 02, 게재확정일 : 2009. 04. 17
* 충주대학교 컴퓨터공학과, ** 충북대학교 전기전자컴퓨터공학부

Ⅰ. 서 론

인터넷의 발전으로 많은 컴퓨터 사용자들이 전자메일, 온라인 쇼핑, 멀티미디어 정보 등과 같은 서비스를 제공하는 인터넷 사용을 생활화하고 있다. HTML 기술을 이용한 웹 기술의 발전은 현대인들의 정보를 빠르고 쉽게 공유할 수 있도록 해주고 있어 그 이용이 기하급수적으로 증가하고 있는 추세이다. 그러나 그에 따른 부작용으로 중요 시스템에 대한 정보 유출, 전산망 침해 등과 같은 침입 행위 또한 빠른 속도로 증가하고 있다[1].

이렇게 급격히 증가하고 있는 침입 행위 공격 중 DDoS 공격은 피해 규모도 크고 탐지하기도 어렵다. 따라서 이러한 DDoS 공격뿐만 아니라 웹에 대한 공격을 조기에 탐지하고 정확하게 탐지하기 위한 새로운 탐지 시스템의 설계가 필요하다. 이러한 요구에 따라 다양한 공격 중 웹에 대한 공격을 탐지하는 방법들이 제안되고 있다. 웹에 대한 공격을 탐지하기 위해 기존에는 프로토콜과 특정 공격 프로그램이 사용하는 포트 번호를 이용하는 방법에 관한 연구가 제안되었다. 그러나 이러한 방법은 정확하게 탐지는 가능하나 탐지 룰에 포함되지 않은 새로운 공격은 탐지 할 수 없다는 문제를 가지고 있다. 또한 유사한 정상 트래픽도 공격으로 간주하는 문제가 발생한다[1-2].

이에 따라 웹에 대한 서비스를 좀 더 안전하게 제공하고 웹 서비스를 이용한 공격을 방어하는 연구의 필요성이 커지고 있다. 더욱이 최근에는 웹 공격에 대해 보다 빠르게 반응할 수 있고, false alarm을 줄일 수 있도록 웹 서비스에 대한 특화된 침입탐지 시스템의 필요성이 급증하고 있다. 웹에 대한 위협 및 공격행위에 대처하기 위해 해결해야 될 중요한 이슈는 어떻게 이상행위를 탐지할 것인가와 탐지된 정보를 어떻게 보고할 것인가의 2가지 큰 이슈가 있다. 이상행위에 대한 탐지는 이미 많은 연구가 이루어지고 있으나 웹의 특성 상 수많은 정보 속에서 관리자가 원하는 정보를 추출하는 것은 쉽지 않다. 이것을 어떻게 효과적으로 추출하고 관리자에게 보고할 수 있는가는 중요한 문제이다[1-3].

이러한 정보를 추출하는 방법들도 초기에는 많이 제안되었으나 보편적으로 오탐율 및 새로운 공격을 탐지 못한다는 문제로 인하여 좀더 개선된 방법이 통계학적 방법을 적용한 방법이다[3]. 본 논문에서 제안하는 공격 트래픽 탐지 기법은 전통적인 네트워크기반 공개 침입탐지시스템(NIDS : Network based Intrusion Detection System)인 Snort를 이용하여 탐지한 공격 트래픽 중 false positive 가능성이 있는 패킷을 Nmap 정보를 이용하여 필터링 하고, nessus 취약점 정보를 이용하여 2차 필터링을 실시한 후, 운영체제의 적합성, 시그너처 위험도, 보안 취약점을 고려한 상관성 분석을 최종적으로 실시하여 false positive 경고 메시지를 줄이고 false positive에 의한 오류를 최소화 하여 전체적인 공격 탐지 결과를 높였다. 이와 같은 특성에 의하여, 본 논문이 제안하는 기법은 기존의 방식에 비하여 짧은 시간에 탐지 및 판단이 이루어짐은 물론 적은양의 공격 트래픽의 탐지도 가능하고 정상 트래픽을 보호할 수 있으며, 한번 탐지된 트래픽에 대해서는 재발 방지를 위한 관리자의 조기 대응이 가능하도록 설계하였다. 그러므로 본 논문에서는 웹 공격에 대하여 false alarm 감축을 위한 효율적인 공격 트래픽 탐지 기법을 이용하여 공격 트래픽 중 false positive 가능성이 있는 패킷에 대하여 공격 탐지를 하여 경고 메시지 및 false positive를 줄일 수 있었으며, 오탐율을 줄이고 탐지 성능을 향상시키는데 최대한 노력을 기울였다.

본 논문의 구성은 Ⅱ장에서는 분산 DoS 공격 탐지에 대하여 기존의 탐지 기법과 기존 공격 탐지 기법의 문제점을 살펴보고, Ⅲ장에서는 본 논문에서 제안한 공격 트래픽 탐지 기법을 통하여 단계별 트래픽에 대한 Snort와 Nmap, Nessus, 그리고 상관성 분석의 필터링을 실시한 후, Ⅳ장에서는 실험과 결과 고찰을 하여 최종적으로 false alarm을 줄이고 탐지성능을 높이는 방안을 제시하고, 마지막으로 Ⅴ장에서는 결론 및 향후 연구 과제를 제시한다.

Ⅱ. 관련 연구

현재 가장 위협적이고 정확한 탐지가 어려운 공격은 DDoS 공격이라 할 수 있다. 본 장에서는 이러한 DDoS 공격을 효율적으로 탐지하기 위해 DDoS 공격 도구의 특징 분석 및 공격을 탐지하기위해 제안되었던 기존 방법에 대해 분석 및 문제점을 기술한다.

1. 분산 DoS 공격 탐지

대부분의 DDoS 공격은 자동화된 툴을 이용하여 에이전트를 확보하고, 다시 확보된 에이전트를 통해서 많은 노드의 슬레이브 시스템을 확보하는 것이 일반적이다. 위의 방법들을 통해서 많은 양의 트래픽을 발생시키고 피해 호스트에 공격을 행하게 되는 것이다. 표 1은 현재 사용하는 DDoS 공격 툴을 비교한 표이다.

표 1. DDoS 공격 툴 비교
Table 1. Comparison of DDoS Tools

종류 / 항목	Trinoo	TFN	Stacheldraht
공격방법	UDP flood	UDP/SYN/ICMP flood, Smurf	UDP/SYN/ICMP flood, Smurf
통신암호화기능	X	X	O
Attacker↔Master	27665/TCP	Telnet 등의 방법	16660/TCP (암호화)
Master↔Agent	27444/UDP	ICMP echo reply	ICMP echo reply, 65000/TCP
Agent↔Master	31335/UDP	ICMP echo reply	ICMP echo reply
IP spoofing 가능	X	O	O
발견 시기	1999년 이전	1999년 이전	1999년 8월
Process Name변경	X	O	O

2. Snort를 이용한 공격 탐지

Snort는 공개용 네트워크 기반 침입탐지시스템으로 실시간 트래픽 분석과 IP 네트워크에서의 패킷 처리작업을 하는 데몬이다. 그리고 프로토콜 분석, 내용 검색·매칭을 수행할 수 있으며 버퍼 오버플로우, Stealth 포트 스캔, CGI 공격, SMB 탐색, OS 확인 시도 등의 다양한 공격과 스캔을 탐지할 수 있다. 또한 트래픽을 분석하며 모듈화된 탐지 엔진을 지원하고 실시간 경고 기능도 지원하는 등 다양하고 복잡한 침입 탐지가 가능하다. Snort의 탐지 룰들은 보안 커뮤니티를 통해 지속적으로 업데이트되고, 사용자가 쉽게 룰을 작성하여 추가할 수 있으므로 최신 공격에 적응이 쉽다. Snort 프로그램은 몇 가지 구성 요소들이 플러그인 형태로 이루어져 있어 쉽게 각자의 환경에 따라 변경하고 수정할 수 있도록 되어 있고, 기본적으로 스니퍼, preprocessor, 탐지 엔진, 알람 및 로깅 정보 출력으로 구성 되어 있다.[4-6]

Snort는 먼저 스니퍼라는 스니핑 툴을 통해 snort IDS를 통과하는 모든 패킷을 수집하고, 여기서 수집된 데이터는 바로 룰 기반의 탐지 엔진을 거치지 않고 그 전에 preprocessor를 통해 보다 효율적인 공격 탐지를 위해 HTTP 인코딩 플러그인이나 포트 스캔 등 몇 가지 플러그인을 먼저 거치면서 매칭이 되는지 확인한다. 그리고 preprocessor를 통과한 패킷은 룰 기반의 탐지 엔진을 거치면서 사전에 정의된 탐지 룰과 매칭되는지 확인한다. 만약 룰에 매칭되었을 경우에는 사전에 정의된 정책에 따라 로그에 남고, 그렇지 않은 경우에는 통과한다.

3. SNMP-MIB를 이용한 공격 탐지

SNMP를 이용한 DDoS 탐지 방법은 관리 객체들의 집합인 MIB(Management Information Base)를 이용하여 트래픽을 수집하고 임계값을 적용하여 유해 트래픽을 분석하는 방법이다[4]. 이러한 방법은 트래픽 수집 단계와 분석 단계로 이루어지며, 트래픽 수집 단계에서는 관리 시스템과 대상 시스템간에 SNMP를 활성화시킨 후, 관리하고자 하는 MIB를 선정하여 정보를 얻게 된다. 관리 시스템과 대상 시스템과의 통신은 SNMP 프로토콜을 통해 주기적인 요청에 의해 해당 정보를 전송하게 된다. 전송된 MIB 정보는 로그 값으로 저장되며 이 값을 토대로 트래픽을 분석하게 된다. 로그 값은 수집된 시간, MIB를 통해 얻어진 트래픽의 평균값, 수집된 트래픽의 최대값으로 저장된다. 이러한 특징을 이용하여 일정기간의 트래픽 정보를 수집하여 임계값을 산출한 후 임계값과 비교하여 DoS 공격을 탐지하는 방법이다. SNMP를 이용한 트래픽 분석의 특징은 유해 트래픽에 대해서 정확한 분석을 할 수 있다는 큰 장점을 가지고 있지만 유해 트래픽을 분석하기 위해 현재의 트래픽량과 이전의 트래픽량을 비교하기 때문에 분석하는데 많은 시간이 소요된다는 단점이 있다. 그림 1은 SNMP를 이용한 기존의 공격 탐지 흐름도이다.[7-8]

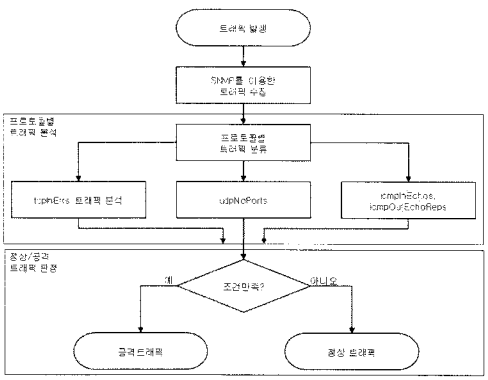

그림 1. SNMP를 이용한 공격 탐지 흐름도
Fig 1. Flow Chart of Used SNMP Detection

4. 기존 공격 탐지 기법의 문제점

Snort를 이용한 탐지 방법은 임계값을 이용하지 않고 공격 시그너처와 사전에 정의된 공격 탐지 룰 파일과의 패턴 매칭 기법을 이용하는 방법으로 불필요한 경고 메시지 발생, 높은 오탐율, 정의된 공격 이외의 탐지 불가 등과 같은 문제가 있다. Snort와 같은 패턴 매칭 기법을 적용하여 탐지하는 방법은 정의된 공격에 한해서는 정확하게 탐지가 가능한 장점이 있지만 정의 되지 않은 공격은 탐지가 불가능한 문제가 있

다. 이로 인해 false negative가 자연 높게 된다. 또한 유사한 시그너처 만으로도 공격으로 간주하여 불필요한 경고 메시지가 발생하게 된다. DDoS의 경우 특정 포트, 특정 데이터 값을 가지는 도구가 존재하므로 이러한 것을 공격 탐지 룰로 세팅하게 된다. 그러나 정상 사용자가 취약점 분석을 위해 포트 스캔을 하더라도 특정 포트에 접근하는 것으로 간주하여 공격으로 판단하는 문제가 발생한다. 현재에도 기존 탐지 방법들의 이러한 문제를 해결하기 위해 많은 연구가 진행되고 있으나 DDoS 탐지 및 방지에 있어 가장 중요한 조건이라 할 수 있는 탐지 시간의 단축, 정확한 판단, 그리고 오탐율의 최소화 등은 아직까지 미흡한 실정이다.

DDoS 공격이 대응하기 어려운 이유 중 가장 심각한 것은 공격자가 발송하는 비정상적인 공격 패킷과 일반 사용자가 사용하는 정상 서비스 요청 패킷을 정확히 구분하는 것이 매우 어렵기 때문에 그 공격 자체를 탐지하기가 힘들다는 것이다. 또한 정확한 탐지가 이루어진다 해도 라우터나 방화벽을 통한 필터링이 어려운 실정이다. 이러한 기법은 아주 정교한 공격에 대해서는 속수무책인 경우가 많고 대응 속도가 너무 느리며 정상적인 서비스 트래픽을 소멸시키는 빈도가 높다. 이러한 문제점은 기존에 DDoS 탐지 방법에서 나타나게 된다. 출발지 IP 모니터링을 이용한 DDoS 탐지 방법은 오탐율이 높다는 점, 네트워크 변동 상황을 고려하지 않는다는 점, 임계값 설정 기준이 모호하다는 점, 특정 DDoS 공격만 탐지한다는 점과 같은 문제가 발생하게 된다. SNMP의 경우 출발지 IP 모니터링을 이용하여 LRU 큐의 빈번한 교체작업의 빈도를 임계값으로 설정하여 공격과 정상 사용자를 구분하는 방법이다. 이로 인한 문제점은 DDoS의 경우 몇몇 도구에서는 모든 패킷들이 동일한 출발지주소로 세팅되어 전송되게 된다. 이러한 경우는 LRU 큐의 교체 작업의 빈도가 임계값을 넘게 되어 공격으로 탐지하게 된다. 그러나 일부 DDoS 도구에서는 출발지주소가 고정이 아니라 랜덤하게 갱신된다. 이러한 경우 출발지 IP를 모니터링하여 탐지하는 방법에서는 공격이 오더라도 LRU 큐의 교체 빈도가 낮기 때문에 공격으로 간주하지 않고 정상으로 간주하는 false negative가 높고 피해가 발생하게 되는 문제가 발생한다. 또한 정상 사용자가 필요에 의해 빈번한 접속을 요구하는 경우도 공격으로 간주하게 되어 false positive율이 높아지는 문제가 있다. SNMP MIB를 이용한 탐지 방법도 유사한 문제가 발생한다. 일반적으로 탐지 작업 수행 시 시스템 과부하가 걸린다는 점, 네트워크에 트래픽이 범람하는 점, 특정 DDoS 공격만 탐지하는 점, 오탐율이 높다는 점 같은 문제점을 가진다.

일반적으로 SNMP의 경우 네트워크 모니터링을 위한 목적으로 많이 사용되었지만, DDoS를 탐지하기 위한 방법으로 연구되어 발표되었다. 이러한 방법은 공격 도구에 의해 생성된 트래픽은 피해 호스트에 응용 프로그램이 존재하지 않기 때문에 특정 MIB 객체에서 반응을 보이게 된다. 이렇게 공격에 반응하는 MIB 객체들을 이용하여 임계값을 설정하게 된다. 이로 인해 대부분의 임계값을 설정하는 탐지 방법과 유사한 false positive, false negative율이 임계값의 설정 유무에 따라 오탐율이 증가하는 문제가 있다. SNMP를 이용한 탐지 방법의 더 큰 문제는 SNMP의 경우 에이전트로부터 트래픽 정보를 가져오기 위해 빈번한 폴링으로 네트워크에 쿼리 트래픽이 범람하여 속도 저하 문제가 발생하고, 여러 에이전트로부터 수집된 데이터 처리에 시스템의 과부하가 발생하게 되는 문제가 발생한다.[5-8]

III. 제안한 트래픽 공격 탐지 기법

본 논문에서 제안하는 공격 트래픽 탐지 기법은 전통적인 네트워크기반 공개 침입탐지시스템(NIDS)인 Snort를 이용하여 탐지한 공격 트래픽 중 false positive 가능성이 있는 패킷을 Nmap 정보를 이용하여 필터링하고, Nessus 취약점 정보를 이용하여 2차 필터링을 실시한 후, 운영체제의 적합성, 시그너처 위험도, 보안 취약점을 고려한 상관성 분석을 하고 최종적으로 경고 메시지를 줄이고 false positive에 의한 오류를 최소화하여 전체적인 공격 탐지 결과는 보안전문가가 아닌 일반 네트워크 관리자가 쉽게 이해하고 대응할 수 있도록 하는 것이다.

1. 제안한 탐지 모델

1.1 설계 목표

본 논문에서 제안하는 상관성을 이용한 공격 트래픽 탐지 분석 시스템의 설계 목표는 크게 4가지로 구성한다.

(1) 패턴 매칭을 이용한 네트워크 공격 탐지 분석
(2) Log file 정규화
(3) 상관성 분석을 통한 공격 판단
(4) 사용자 관점의 공격 탐지 출력

최종적으로 공격으로 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 공격 탐지 비율을 화면에 출력한다.

1.2 프로세스 흐름도

본 논문에서 제안하는 프로세스 흐름도는 그림 2와 같다. 네트워크상의 모든 패킷은 snort 기반의 NIDS에 의해 패턴 매칭을 실시하고 각각의 패킷에 대한 위험도에 따라 데이터베이스에 저장되며, 웹에 전달된 패킷의 처리 결과를 분석하여 정규화 형태로 데이터베이스에 전달한다. 상관관계 분석 모듈은 각각의 결과를 읽어 최종 공격인지 판단하여 결과를 실시간으로 사용자에게 출력하여 전달한다.

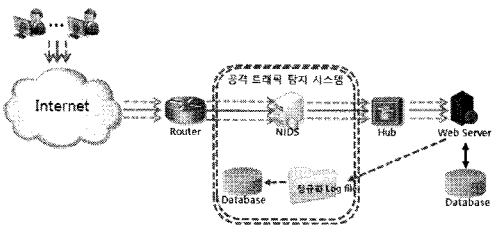

그림 2. 프로세스 흐름도
Fig 2. Flow Chart of Process

1.3 시스템 구현

본 논문에서 구현한 시스템은 그림 3과 같이 우선 공격 트래픽과 일반 트래픽을 따로 데이터베이스에 저장한다.

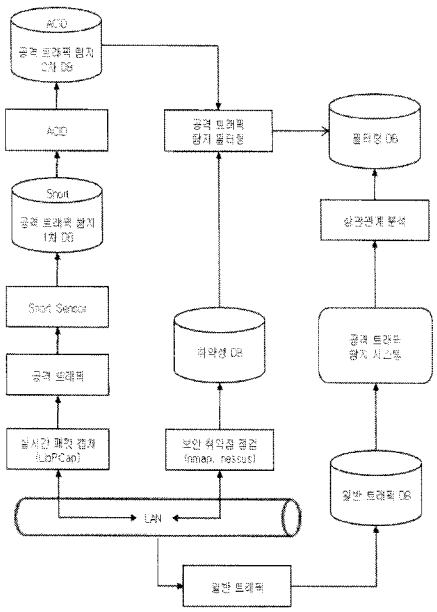

그림 3. 공격 트래픽 탐지 분석 시스템 구조
Fig 3. Structure of Attack Traffic Detection analysis

2. 경고 메시지의 상관성 분석

경고 메시지의 상관성 분석은 침입탐지 트래픽이 기존의 침입 트래픽과 어느 정도 상관관계가 있는지 조사하여 경고 메시지를 최소화하는 기법이다. 경고 메시지의 최소화를 위한 기존 연구 방법으로 유사성에 기초한 확률적인 방법, 정의된 공격 상태 그룹에 의한 ACC 방법, 그리고 공격의 전제조건을 이용한 유사성 평가 방법이 있다[3].

2.1 유사성에 기초한 확률적인 방법

이 기법은 경고 메시지 사이의 유사성을 베이지언(Bayesian) 통계에 의한 확률적 방법으로 구해 비슷한 경고 메시지들을 그룹화하여 경고 메시지를 최소화하는 방법으로 EMERALD에서 활용되고 있는 기법이다.

서로 다른 센서들의 침입탐지 메시지들을 교환하기 위한 침입탐지시스템의 유형, 위치, 공격 목표, 비정상 필드를 담고 있는 경고 메시지 템플릿을 고려하여 새로운 경고 메시지와 기존 메타 경고 메시지를 비교한 후 확률값인 0과 1사이의 값을 반환하는 적합한 유사성 함수를 정의하여 사용한다. 전체 유사성은 특징 유사성들의 가중 평균으로 구하며 새로운 경고 메시지가 기존의 메타 경고 메시지와 비슷할 경우 같은 그룹으로 묶여지며 그렇지 않을 경우 새로운 경고 메시지는 새로운 메타 경고 메시지 쓰레드를 생성하여 다음 경고 메시지와 비교한다. 이 기법은 경고 메시지 사이의 인과관계를 발견하기 곤란하며 유사성이 낮은 공격을 탐지하기 어렵다는 문제점을 가지고 있다.

2.2 정의된 공격 상태 그룹에 의한 ACC 방법

ACC(Aggregation and Correlation Component)는 여러 침입탐지시스템인 probe로부터 경고 메시지를 획득한 후 중복, 연속된 것은 동일한 공격 유형 상관관계로 판단하고 출발지주소, 목적지주소, 공격의 유형에 따라 7가지 상태 그룹관계로 판단하여 관리자에게 농축된 경고 메시지 결과를 제공한다. 이 기법은 IBM/Tivoli TEC에서 사용하는 것으로 미리 정의된 공격 상태 그룹별로 유사성을 판단, 경고 메시지를 최소화하는 방법이다. 경고 메시지 클래스 계층은 probe가 탐지한 경고 메시지의 기본 정보를 담고 있는 probe 계층, 목적지주소 정보를 담고 있는 target 계층, 출발지주소 정보를 담고 있는 source 계층, 세부적인 서비스 정보를 담고 있는 detailed target 계층으로 구분된다. 이 기법은 미리 정의된 공격 상태 그룹에 해당하지 않는 공격이 있을 경우 문제점이 발생한다.

2.3 공격의 전제조건을 이용한 유사성 평가 방법

이 기법은 공격의 전제조건을 이용하여 경고 메시지의 유사성을 평가하는 방법으로 특정 사전 공격은 사후 공격을 위한 준비 단계라는 것을 이용한다. 그림 3-4와 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 4는 (c)와 같은 DDoS 공격의 상관관계 그래프가 존재할 경우 (a)와 같은 특정 네트워크에 존재하는 호스트를 발견하기 위한 IP Sweep 사전 공격과 (b)와 같은 뒤이은 버퍼 오버플로우 공격이 같은 공격 형태로 판단될 수 있음을 의미한다.

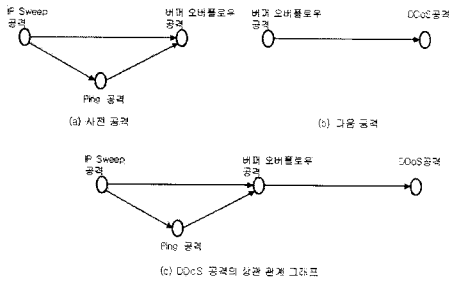

그림 4. 공격의 전제 조건을 이용한 상관관계 그래프
Fig 4. Correlation graph of used Precondition

3. Snort를 이용한 공격 탐지

Snort는 네트워크상에서 실시간 트래픽 분석과 패킷 로깅을 수행하는 작고 가벼운 네트워크 침입 탐지 도구이다. Snort는 특히 프로토콜 분석과 패킷의 내용 조사, 패턴 매칭이 가능하며, 버퍼 오버플로우나 스텔스, 포트 스캔, CGI 공격 등 다양한 공격을 탐지할 수 있다. 또한 최근 많이 대두되고 있는 DDoS 공격에서는 패턴 매칭 기술을 이용하여 탐지가 가능하다. Snort는 수집된 데이터를 이용하여 패턴 매칭 기법을 이용함으로써 사전에 정의된 DDoS 공격에 대해서는 정확한 탐지가 가능하나 DDoS와 유사한 정상 패킷에 대해서는 오탐율이 비교적 큰 단점이 있다. Snort 자체가 DDoS 공격만을 위한 침입 탐지 도구가 아니기 때문에 DDoS 공격에 대한 공격 시그너처의 개수가 적어 시그너처를 보유하지 않은 공격에 대해서는 탐지 할 수 없다는 단점을 가지고 있다.

4. Nmap 정보를 이용한 1차 필터링

본 논문에서는 ACID가 생성한 공격 트래픽 탐지 2차 데이터베이스 중 불필요한 경고 메시지나 false positive 오류의 가능성이 있는 경고 메시지를 제거한다.

그 방법으로는 우선 감시하고자 하는 호스트들을 Nmap과 Nessus를 이용하여 보안 취약점 점검을 한다. 그 후 보안 취약점 점검으로 인해 생성된 취약점 데이터베이스와 2차 공격 트래픽 탐지 데이터베이스를 비교하여 불필요한 데이터를 필터링한다. 마지막으로 생성된 필터링 데이터베이스의 자료 중 동일한 목적지주소, 포트번호, 공격유형별로 그룹화하고 상관분석 작업을 진행한다. 상관관계 분석작업은 운영체제의 적합성, 시그너처의 위험도, 보안 취약성 정도를 고려하여 지정한 임계치를 초과할 경우 공격 트래픽으로 최종 판단을 내리고 웹상에서 일반 트래픽과 공격 트래픽으로 구분하여 프로토콜별, 서비스별, IP별로 네트워크 관리자에게 보여준다. 그림 5에서 일반 트래픽 처리는 LibPCap과 MySQL연동을 통하여 감시하고자 하는 네트워크의 패킷만을 캡쳐한다.

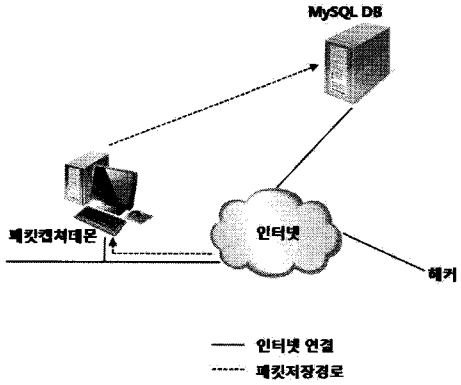

그림 5. 패킷 캡쳐 프로그램 구성도
Fig 5. Program Structure of Packet Capture

공격 트래픽은 Snort의 탐지 룰에 의거하여 탐지되며 탐지된 결과는 MySQL snort 데이터베이스에 저장된다. 본 논문에서 이용하는 ACID의 acid_event 테이블의 내용은 snort의 event 테이블 필드인 sid, cid, signature, timestamp 필드에 ACID가 자체적으로 참고한 필드가 들어 있으며 각각의 필드는 다른 테이블과 sid, cid 필드를 이용하여 연결되어 있다.

Snort는 기능이 막강한 반면 너무 많은 경고 메시지가 관리자 화면에 나타난다. 따라서 false positive 오류로 판단할 수 있는 공격 트래픽 탐지의 필터링이 필요하다. 본 논문에서는 필터링을 2단계로 실시한다. 1차적으로 공격 트래픽 탐지의 목적지주소 및 포트번호, IP 프로토콜을 감시 대상 호스트

들과 비교하고, 2차적으로 보안 취약성 검사의 결과와 비교하여 false positive 오류 가능성이 있는 트래픽을 필터링한다. 공격 트래픽 탐지의 목적지주소 및 포트번호, IP 프로토콜을 검사하여 IP 프로토콜이 TCP/UDP일 경우 감시 대상 호스트들이 실제로 해당 포트를 열어놓고 있는지 검사하여 그렇지 않은 공격 트래픽 탐지들을 필터링한다. 그림 6과 같이 목적지주소 및 포트번호, IP 프로토콜은 서비스되고 있지 않는 포트를 통한 공격을 필터링 하는데 유용하게 사용된다.

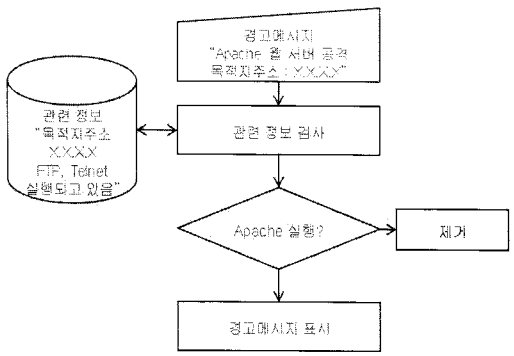

그림 6. 공격 트래픽 탐지 필터링 구조
Fig 6. Filtering structure of Attack Traffic Detection

필터링 과정은 acid_event 테이블로부터 공격 트래픽 탐지를 읽어온 후 해당 트래픽이 TCP/UDP일 경우 감시 대상 호스트에서 실제로 서비스되고 있는 내용을 담고 있는 ports_open 테이블의 내용과 비교한다. 만약 목적지주소, 포트번호가 동일하지 않는다면 해당 트래픽 정보를 제거한다.

5. Nessus 정보를 이용한 2차 필터링

공격 트래픽 탐지 1차 필터링은 공격 트래픽 탐지의 IP 프로토콜이 TCP/UDP이고 목적지주소 및 포트가 감시 대상 호스트와 일치하지 않을 경우 필터링 하는 것이었다. 하지만 공격은 TCP/UDP 이외에 ICMP를 사용할 수도 있고 IP프로토콜이 TCP/UDP 이더라도 감시 대상 호스트가 해당 공격에 취약성을 보이지 않을 경우도 있다. 이러한 경우가 공격 트래픽 탐지 2차 필터링 대상이 된다. 공격 트래픽 탐지 2차 필터링에서는 Nessus를 이용한다. NessusWX를 이용하면 Nessus를 이용한 취약점 점검 결과를 MySQL 데이터베이스에 저장할 수 있다. 2차 필터링은 service, type 필드를 참고하여 목적지주소, 프로토콜, 포트번호가 동일하지 않거나 위험도를 나타내는 type이 2 이상인 것 이외의 공격 트래픽 탐지 정보를 필터링한다. 이 경우 프로토콜과 포트번호가 service라는 필드에 같이 있으므로 비교하기가 까다롭다. 따라서 그림 7과 같이 프로토콜과 포트번호를 따로 저장하는 프로그램을 작성하여 그 결과인 nessus_results 테이블의 정보를 이용하여 공격 트래픽 탐지 2차 필터링을 한다. 여기서 host는 감시대상 호스트, port는 열려져 있는 포트, service는 IP 프로토콜 유형, type은 NessusWX가 판단한 위험도이다.

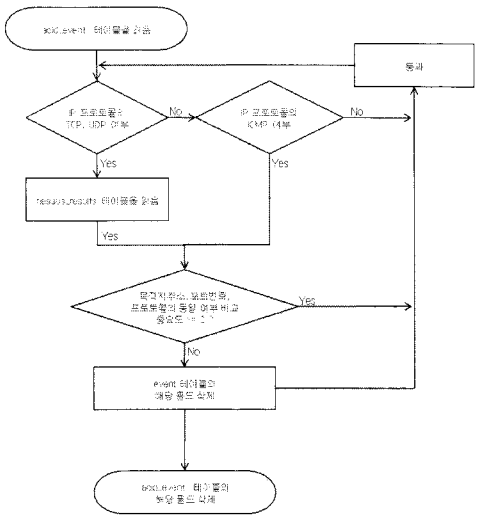

그림 7. 공격 트래픽 탐지 2차 필터링 구조
Fig 7. 2'nd Filtering structure of Attack Traffic

6. 상관성 분석에 의한 최종 판단

6.1 상관성 분석

본 논문에서 제안하고 있는 공격 트래픽 탐지의 상관성 분석은 운영체제의 적합성, 시그너처 위험도, 보안 취약점 정도를 고려한다. 공격 트래픽 탐지 중 동일한 목적지주소, 포트번호, 공격유형별로 그룹화 한 후 각각의 공격 트래픽 탐지의 상관관계를 분석한다. 운영체제 적합성 검사는 공격 트래픽 탐지 중 대부분이 운영체제 종속성을 보이고 있다는 것을 이용한 것이다. acid_event 테이블 중 signature 필드를 이용, signature 테이블에서 sig_sid를 얻을 수 있는데 이것은 Snort 침입 탐지 룰의 내부 시그너처 ID이다. 예를 들어 sig_sid 112가 의미하는 것은 백도어인 BackOriffice2k가 접근하는 것으로 이 룰은 Windows 95/98/ XP/NT에만 영향을 미친다. 시그너처 위험도 검사는 Snort에서 탐지한 시그너처의 우선순위가 1인 경우 위험, 2인 경우 보통, 3 이상인 경우 낮음을 이용한 것이다.

보안 취약점 정도 검사는 Nessus에서 판단을 내린 중요도의 값을 이용하는 것으로 0, 2 또는 3의 값을 갖는다. 0은 단

순히 해당 포트가 열려 있음을 뜻하고, 2는 보통, 3은 취약성을 내포하고 있음을 나타낸다. Backdoor 공격 툴인 NetBus, BackOriffice2K와 DDoS공격 툴인 Trinoo, TFN, Stacheldraht 공격도구를 사용하여 테스트 한 결과 표 2와 같은 비교항목간 상관성 비율을 구하였다. 이 결과에서 공격 트래픽 탐지가 운영체제에 종속적임을 알 수 있었으며 시그너처의 위험도 및 Nessus의 취약점 정도 또한 공격과 상당한 상관성이 있음을 알 수 있었다. 이것을 근거로 본 논문에서는 수식 (3-1)와 같은 공격 트래픽 탐지 상관성 판단 기준을 제안 한다. 제안 이유는 시그너처의 위험도 중 1인 경우와 Nessus의 취약점 중 3인 경우가 관심사항이기 때문이다.

협력적 필터링의 일반적인 형태로 피어슨 상관계수가 사용된다.

표 2. 비교 항목의 상관성 비율
Table 2. Ratio Correlation of Comparison Item

구 분	비교 항목								
공격 툴	경고 메시지 수	운영체제의 적합성		시그너처의 위험도			Nessus 취약점 정도		
		일치	불 일치	1	2	30|상	3	2	1
Netbus, BO2K 각 10회 공격	6	6 (100%)	0 (0%)	3 (50%)	0 (0%)	3 (50%)	6 (100%)	0 (0%)	0 (0%)
Trinoo, TFN, Stacheldraht 각 5초간 공격	3905	3905 (100%)	0 (0%)	0 (0%)	47 (1.2%)	3858 (98.8%)	27 (0.7%)	16 (0.4%)	3862 (98.9%)
총 비율		100%	0%	25%	0.6%	74.4%	50.35%	0.2%	49.45%

$$P_{a,j} = \overline{v_a} + \frac{\sum_{j=1}^{n} w(a,i)(v_{i,j} - \overline{v_i})}{\sum_{i=1}^{n} w(a,i)} \quad (3\text{-}1)$$

여기서, Pa,j : 사용자 a의 아이템 j에 대한 선호도를 예측한 값,

$\overline{v_a}$: 사용자 a의 선호도 평균값,

$w(a,i)$: 사용자 a의 사용자 i와 사용자 i의 유사도 가중치,

n : 사용자 a와 다른 사용자간의 유사도가 0이 아닌 사용자 수,

$w(a,i)$: 사용자 a와 i의 유사도 가중치이다.

공격 트래픽 탐지 상관성 판단 순서도는 그림 8과 같으며 상관성 판단 기준에 의한 점수를 고려하여, 또한 취약점 정보와 시그너처 위험도, 보안 취약점 등을 전체적으로 살펴보았을 때 총합이 1과 2 사이인 1.3이상일 때의 경우를 최종 공격 트래픽으로 판단한다.

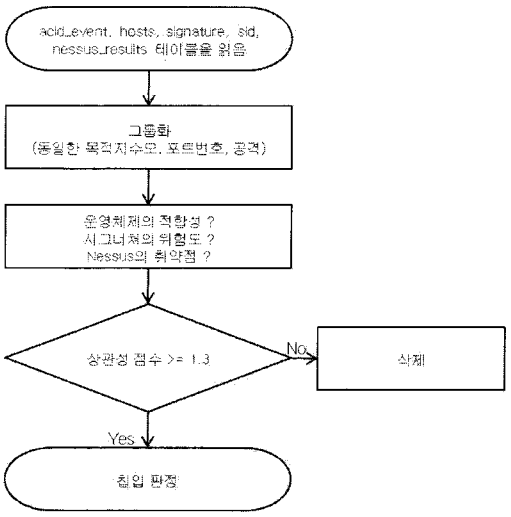

그림 8. 공격 트래픽 탐지 상관성 판단 구조
Fig 8. Correlation judgment Structure of Attack Traffic Detection

6.2 구현과정

본 논문에서 제안한 False Alarm 감축을 위한 효율적인 공격 트래픽 탐지 분석 시스템의 구현 과정은 다음과 같다. 우선 Snort가 탐지한 공격 트래픽 탐지 중 false positive 오류 가능성이 있거나 중요도가 낮은 패킷을 nmap의 결과인 열려 있는 포트 정보를 이용하여 1차 필터링을 하고, nessus 취약점 정보를 이용하여 2차 필터링 과정을 거치면서 제거했다. 그 후 필터링 된 공격 탐지 패킷 중 최종 공격 트래픽으로 판단하기 위한 상관관계 분석 과정을 진행했다. 진행 과정은 크론 데몬을 이용하여 주기적으로 실행을 하였다.

VI. 실험 및 결과 고찰

본 논문에서 제안한 False Alarm 감축을 위한 효율적인 공격 트래픽 탐지 분석 시스템의 성능을 평가하기 위하여 일정기간 동안 수집된 네트워크 트래픽과 공격 프로그램으로 생성된 트래픽을 기반으로 Snort가 탐지한 공격 트래픽 데이터베이스 분석 엔진인 ACID와 제안한 시스템을 비교하여 경고 메시지 수 및 false positive 오류율을 각각 비교 분석하였다. 실험은 6가지 공격기법과 2008년 4월 21일부터 4월 30일까지 10일 동안 수집된 패킷 자료를 기반으로 하였다.

1. 시스템 구성

테스트 베드의 전체적인 구성은 그림 9와 같이 Snort(ACID)와 웹 기반의 공격 트래픽 탐지 분석 시스템이 같은 서버에 존재하며 클라이언트에서 공격 트래픽 탐지 분석 결과를 웹브라우저를 통해 확인하게 하였다. 그리고 공격은 인터넷을 통한 공격시스템의 외부 공격과 실험을 위한 공격용 PC에서 내부 공격을 하게 하였다.

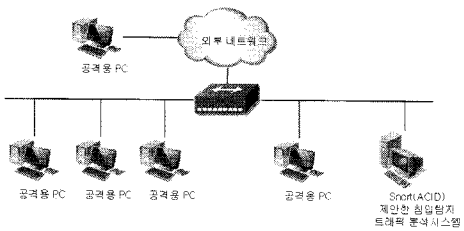

그림 9. 실험 환경 구성도
Fig 9. Test Bed

성능 평가를 위한 공격 프로그램은 표 3과 같다.

표 3. 공격 프로그램
Table 3. Program of Attack Tools

공격 프로그램	공격 유형	취약 시스템	공격 방법
NetBus, BackOriffice2K	NetBIOS을 통한 공유 폴더 암호 크랙	Windows 95/98/Me/ XP/NT/2000/2003	10회
Linux rootkit	Trojan	리눅스계열	10회
Trinoo, TFN, Stacheldraht	DDoS공격	유닉스계열	5초

2. 결과 고찰

본 논문에서는 제안한 False Alarm 감축을 위한 효율적인 공격 트래픽 탐지 분석 시스템에 대한 false positive 오류율을 Snort(ACID)와 비교한 결과 표 4와 같이 제안한 모델이 21.37%정도 우수함을 알 수 있었다.

표 4. 제안 모델의 성능 비교
Table 4. Proposal Model's performance comparison

비교 항목	탐지패킷	정상패킷	침입패킷	false positive
snort(ACID)	4,681개	2,730개	2,351개	68.29%
제안시스템	1,911개	691개	1,221개	46.92%

또한 제안 모델의 필터링 및 상관관계 분석 과정별 경고 메시지의 변화 결과를 2008년 4월 21일부터 4월 30일(10일간)까지 수집된 패킷의 평균을 기준으로 살펴본 결과 표 5와 같이 91.3%의 경고 메시지 감소 효과를 볼 수 있었으며, 약 8.70%에 대한 Side effect가 있는 것을 또한 알 수 있었다..

표 5. 경고 메시지 비교
Table 5. Warning Message Comparison

제안 시스템 과정	경고 메시지 수	감소비율
Snort(ACID)탐지 후	52,821개	
1차 필터링 후	10,565개	80.01%
2차 필터링 후	6,688개	87.34%
상관성 분석 후	4,596개	91.30%

그림 10은 전체 패킷 중 10일간의 false positive alarm의 메시지 변화량을 Snort(ACID) 탐지 후와 1차 필터링 후를 비교한 결과이다. 그림 11은 Snort(ACID) 탐지 후와 2차 필터링 후를 비교한 결과이고, 그림 12는 Snort(ACID) 탐지 후와 상관성 분석 후를 비교하여 각각의 경고 메시지의 변화량에 대하여 분석한 결과이다.

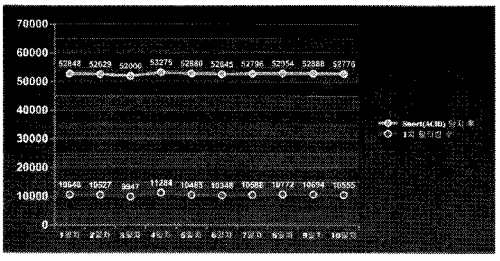

그림 10. Snort와 1차 필터링 후 경고 메시지 변화
Fig 10. 1'st Warning Message Monitoring

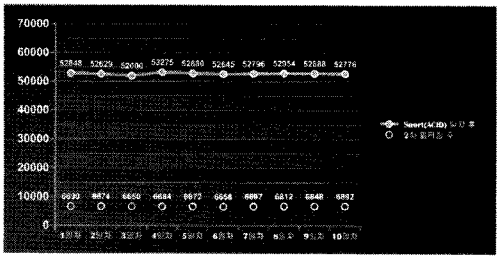

그림 11. Snort와 2차 필터링 후 경고 메시지 변화
Fig 11. 2'nd Warning Message Monitoring

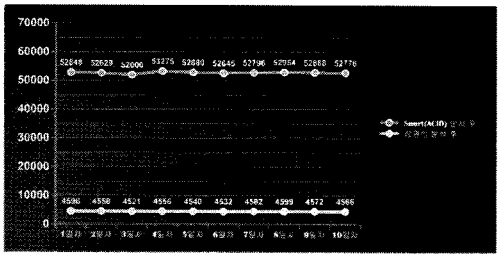

그림 12. Snort와 상관성 분석 후 경고 메시지 변화
Fig 12. Warning Message Monitoring of Correlation analysis

실험 결과 표 6과 같이 보안 대상 호스트 프로토콜별, IP별로 공격 트래픽 탐지 현황을 파악할 수 있으며 특히, 서비스별로 공격 트래픽을 구분할 수 있어 현재 어떤 공격이 있었는지에 대한 단서를 찾을 수 있었다. 그리고 공격 트래픽 탐지 비율을 전체 트래픽과 비교할 수 있었으며 공격 트래픽이 많이 발생한 IP를 사용자에게 알려줌으로써 보안의 필요성을 확연히 설명해 줄 수 있는 계기를 마련할 수 있었다.

표 6. 제안 모델의 기능
Table 6. Proposal Model's Performance

비교 기능	Snort(ACID)	제안 모델
프로토콜별 표시	○	○
서비스별 표시	○	○
IP별 표시	○	○
침입탐지 트래픽 비율 표시	×	○
히스토리	○	○

V. 결론

해킹·바이러스의 지능화, 금융 사기의 증가, 정보 유출, 전산망 침해 등 정보화 역기능이 두드러지게 나타나고 있는 요즘 보안의 중요성 및 필요성이 점차 중요시되고 있다. 하지만 보안관련 회사 및 대기업을 제외하고는 보안전문가가 아닌 일반 관리자가 시스템 및 네트워크를 관리하고 있는 상태이다.

또한 기존의 Snort와 같은 침입탐지시스템은 수없이 많은 경고 메시지를 관리자의 화면상에 표시함으로써 해당 관리자를 혼란에 빠트려 해킹 초기 대응능력을 무력하게 만드는 문제점과 함께 침입탐지시스템의 잘못된 환경 설정으로 인한 false positive 오류 가능성을 내포하고 있다.

이에 본 논문에서는 경고 메시지를 줄이고 공격 트래픽을 효율적으로 탐지하기 위한 방법으로 네트워크 기반의 IDS인 Snort, Nmap, Nessus의 정보를 이용하여 false positive rate의 감소를 위해 Snort(ACID)를 이용하여 공격 탐지를 실시했다. 또한 TCP와 UDP에서의 Nmap, Nessus의 정보를 이용하여 1차, 2차 필터링을 실시하였고, 최종적으로 운영체제의 적합성, 시그너처 위험도, 보안 취약점을 고려한 상관성 분석을 통하여 공격 트래픽으로 판단하는 공격 트래픽 탐지 기법을 제안하였으며 트래픽을 일반 트래픽과 공격 트래픽으로 분류하고, 각각의 트래픽을 프로토콜별, 서비스별, IP별로 구분하여 관리자가 전체적으로 공격 트래픽 탐지 상황을 웹브라우저 상에서 쉽게 확인할 수 있도록 구현하였다. 구현된 시스템에서 상관성 분석을 이용한 공격 트래픽 탐지 기법 결과 경고 메시지 및 false positive를 줄일 수 있었으며 해커에 의한 외부 공격이 발생할 경우 관리자의 초기 대응 능력 기술 향상을 기대할 수 있었다. 특히 공격 트래픽이 많이 발생한 IP를 사용자에게 알려줌으로써 보안의 필요성을 확연히 인식하게 할 수 있는 계기를 마련하였다. 향후 연구 과제로는 웹 공격에 대한 통합 보안 관리(ESM)에 대한 연구와 경고 메세지를 효율적으로 관리할 수 있는 히스토리 기능 및 검색 기능을 강화하여 관리자의 신속 정확한 대응 능력 강화 기법에 대한 연구가 필요하다.

참고문헌

[1] OWASP. vulnerability, *http://www.owasp.org/index.php/OWASP:About*

[2] S. Kumar, "Classification and Detection of Computer Intrusion", Department of Computer Sciences, Purdue University, PhD Dissertation, Coast TR 95-08, 1995.

[3] A. Valdes and K. Skinner, "Probabilistic alert correlation", RAID 2001, pp 54-68, 2001.

[4] Jonatan Gomez, Fabio Gonzakez, Dipankar Dasgupta, "An Immuno-Fuzzy Approach to

Anomaly Detection" in Proc. IEEE, 2003.
[5] Snort Signature Database, *http://www.snort.org/snort-db/sid.html?sid=112*
[6] 신현준, 최일준, 추병균, 오창석 "웹 트래픽 분석을 통한 유해 트래픽 탐지", 한국컴퓨터정보학회 논문지, 제12권 제2호, 221-229쪽, 2007년 5월.
[7] 장문수, 오창석 "트래픽 분석에 의한 웹 어플리케이션 공격 방지", 한국컴퓨터정보학회 논문지, 제13권 제3호, 139-146쪽, 2008년 5월.
[8] 한순재, "상관성을 이용한 웹 기반의 침입탐지 트래픽 분석", 충북대학교 대학원, 석사학위논문, 2004년 2월.
[9] 최일준, 구경옥, "상관성을 이용한 웹 공격 탐지 기법", 한국엔터테인먼트산업학회 2008년 춘계학술대회 논문집, 70-73쪽 2008년 5월.
[10] 홍성민, 최일준, 추병균, 오창석 "사용자 인증과 파라미터 암호화를 이용한 웹 공격 차단 알고리즘", 한국엔터테인먼트산업학회 논문지, 제1권, 제1호, 54-59쪽, 2007년 12월.
[11] A. Valdes and K. Skinner, "Probabilistic alert correlation", RAID 2001: pp. 54-68, 2001.
[12] H. Debar and A.Wespi, "Aggregation and correlation of intrusion-detection alerts", In Recent Advances in Intrusion Detection, 2001.
[13] P. Ning and Y. Cui, "An intrusion alert correlator based on prerequisites of intrusion", North Carolina State University, January 2002.
[14] C. Schuba, I. Krsul, M. Kuhn, E. Spafford, A. Sundaram, D. Zamboni. "Analysis of a Denial of Service Attack on TCP", Proc. of the IEEE Symp, on Security and Privacy: pp. 208-223, 1997.
[15] R. Stone, "An IP Overlay Network for Tracing DoS Floods", in Proc. 2000 USENIX Security Symp, 2000.
[16] D. Dittrich, "*Distributed Denial of Service Attacks/tools Resource Page*" University of Wasington, 2000.

저 자 소 개

최 일 준

1997년 2월 충주대학교 컴퓨터공학과 (공학사)
2003년 8월 충북대학교 전기전산공학과(공학석사)
2008년 8월 충북대학교 컴퓨터공학과(공학박사)
2005년 3월 ~ 2009년 2월 충주대학교 컴퓨터공학과 겸임교수
2009년 3월 ~ 현재 충북대학교 전기전자컴퓨터공학부 초빙교수
〈관심분야〉 : 정보보안, 네트워크보안

추 병 균

1999년 2월 충주대학교 컴퓨터공학과 (공학사)
2004년 8월 충북대학교 전기전산공학과(공학석사)
2005년 3월 ~ 현재 충북대학교 컴퓨터공학과 박사과정 수료
〈관심분야〉 : 정보보안, 네트워크보안

오 창 석

1978년 2월 연세대학교 전자공학과 (공학사)
1980년 2월 연세대학교 전자공학과 (공학석사)
1988년 8월 연세대학교 전자공학과 (공학박사)
1985년 ~ 현재 충북대학교 전기전자컴퓨터공학부 교수
1982년 ~ 1984년 한국전자통신연구소 연구원
1990년 ~ 1991년 Stanford대학교 객원교수
2007년 8월 ~ 현재 충북대학교 전산정보원장
2007년 7월 ~ 현재 한국엔터테인먼트산업학회 회장
〈관심분야〉 컴퓨터네트워크, 뉴로컴퓨터, 정보보호