韓國 컴퓨터情報學會 論文誌
第9卷 第4號, 2004. 12.

2004-9-4-3-3

상호연관성 분석을 이용한 웹서버 보안관리 시스템 *

김 성 락**

Web-Server Security Management system using the correlation analysis

Sung-Rak Kim**

요 약

본 논문에서는 현재 증가하고 있는 웹 서비스 공격을 정확하고 빠르게 탐지할 수 있고, 잘못된 공격탐지를 줄여줄 수 있는 웹서버 보안관리시스템을 제안한다. 이 시스템은 여러 단위보안모듈들의 결과를 실시간으로 수집하고 상호연관성 분석과정을 통해 탐지의 정확성을 향상시킨다. 단위보안모듈은 네트웍기반 침입탐지시스템 모듈, 파일무결성 검사 모듈, 시스템로그분석 모듈 그리고 웹로그분석 모듈로 구성되며, 그리고 각각의 단위보안모듈들의 결과에 연관성을 부여하여 실시간으로 분석하는 상호연관성 분석 모듈이 있다. 제안한 시스템은 공격탐지의 정확성 뿐 아니라 단위보안모듈의 추가 그리고 상호연관성 분석의 범위 확장이 용이한 프레임워크를 제공한다. 그리고 제안한 시스템의 단위보안모듈 중 침입탐지시스템 모듈은 다중 쓰레드 기반으로 Snort를 재구성하여 보다 빠른 공격 탐지 시간을 갖는다. 처리량이 많은 단위보안모듈의 처리시간을 단축함으로서 웹서버 보안관리시스템 처리 성능을 향상시킬 수 있다.

Abstract

The paper suggests that web-server security management system will be able to detect the web service attack accurately and swiftly which is keeping on increasing at the moment and reduce the possibility of the false positive detection. This system gathers the results of many unit security modules at the real time and enhances the correctness of the detection through the correlation analysis procedure. The unit security module consists of Network based Intrusion Detection System module, File Integrity Check module, System Log Analysis module, and Web Log Analysis and there is the Correlation Analysis module that analyzes the correlations on the spot as a result of each unit security module processing. The suggested system provides the feasible framework of the range extension of correlation analysis and the addition of unit security module, as well as the correctness of the attack detection. In addition, the attack detection system module among the suggested systems has the faster detection time by means of restructuring Snort with multi thread base system. WSM will be improved through shortening the processing time of many unit security modules with heavy traffic.

▸ Keyword : NIDS, Snort, Intrusion Detection, Correlation

• 제1저자 : 김성락
• 접수일 : 2004.09.27, 심사완료일 : 2004.11.13
* 본 논문은 오산대학 산업기술연구소의 학술비지원금에 의한 연구실적물 임.
** 오산대학 인터넷정보관리과 부교수

쓰레드 기반으로 Snort를 재설계하여 탐지시간을 빠르게 향상시킬 수 있다. 처리량이 많은 단위보안모듈의 처리시간을 단축시켜서 결과적으로 웹서버 보안관리시스템 처리 성능을 향상시킬 수 있다.

I. 서 론

인터넷의 발달은 생활의 편리함뿐 만 아니라 컴퓨터 범죄, 해킹 등과 같은 역기능을 증가시키고 있다. 이러한 역기능을 막기 위해 여러 단위보안제품이 개발되고 연구되어지고 있다[1]. 단위보안제품 중 방화벽을 이용하면 다음과 같은 기능으로 보안을 향상시킬 수 있다. 웹 서비스인 80번 HTTP 포트만 열어 서비스하고 나머지 다른 모든 포트는 막는 것이다. 이런 방법은 많은 외부 해킹 공격을 막을 수 있다. 그러나 웹 서비스를 위해 열어놓은 80번 포트를 이용해 공격 한다면 방어할 수가 없다. 다른 단위보안제품으로 네트워크기반 침입탐지시스템(NIDS: Network based Intrusion Detection System)이 있는데, 이는 들어오고 나가는 패킷을 감시하여 미리 정의된 침입패턴(signature)에 의해 공격을 탐지한다. 이 시스템은 정의된 공격만 탐지할 수 있고 정의되지 않은 공격은 탐지 할 수 없으며 또한 실제 공격이 아닌 동일한 패턴에 대해서도 잘못 탐지 할 수 있다[5][7]. 즉, 단위보안제품들은 모두 기능의 범위와 특성이 다르며 상호 보완적인 성격을 갖는다. 보안기능의 향상을 위해서는 여러 단위보안제품들을 이용할 수밖에 없다. 이러한 단위보안제품 모두를 이용한다면 비용과 관리의 증가가 필수적이다.

본 논문에서는 웹 서비스와 같은 특정 시스템에 대해서 비용과 관리의 증가 없이 정확하고 빠르게 공격을 탐지 할 수 있고, 잘못된 공격탐지를 줄일 수 있는 웹서버 보안관리시스템(WSM : Web-Server Security Management, 이하 WSM)을 제안한다.

이 시스템은 비용절감 효과를 위해 공개 소스 기반의 단위보안 제품을 이용하며 다음의 4가지의 단위보안모듈로 구성된다. 네트웍기반 침입탐지시스템 모듈, 파일무결성 검사 모듈, 시스템 로그분석 모듈 그리고 웹 로그분석 모듈로 구성된다. 그리고 관리적인 측면에서 상호연관성 분석 모듈을 이용한다. 이 모듈은 여러 단위보안모듈들의 결과에 연관성을 부여하여 실시간으로 분석한다. 그리고 공격탐지의 정확성 뿐 아니라 모듈의 추가, 상호연관성 분석 범위 확장이 용이하도록 프레임워크를 구성한다. 또한 제안한 시스템의 단위보안모듈 중 네트웍기반 침입탐지시스템 모듈은 다중

II. 관련 연구

본 논문에서 주 기능을 담당하는 단위보안모듈이 네트웍기반 침입탐지시스템이다. 먼저 공개소스인 표준 Snort에 대해 알아보고, 이를 수정한 다중 쓰레드 기반의 Snort 시스템과 그리고 본 논문에서 제안한 웹서버 보안관리시스템의 핵심기능인 상호연관성분석 개념에 대해 알아본다.

2.1 Snort 시스템

Snort는 네트웍기반 침입탐지시스템으로 실시간 트래픽 분석과, IP 네트워크에서의 패킷 처리작업을 하는 데몬이다. 그리고 프로토콜 분석, 컨텐츠 검색/조합 작업을 할 수 있으며, 버퍼 오버플로우, 스텔스 포트스캔, CGI 공격 등 다양한 네트웍 공격을 감지할 수도 있다. 또한 Snort는 트래픽을 분석하며 모듈화 된 탐지 엔진을 지원하고 실시간 경고 기능도 지원하는 등 다양하고 복잡한 침입 탐지가 가능하다.

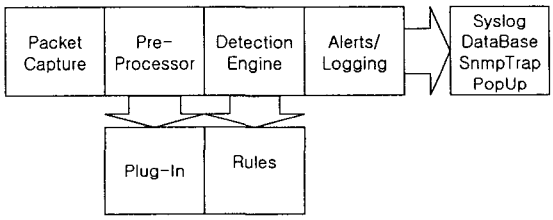

그림 1. Snort 시스템 구조
Figure 1. Architecture of Snort system

(그림 1)과 같이 Snort의 구조는 단일 프로세스로 패킷 캡쳐 후 선행처리와 침입패턴 비교에 의한 탐지 단계, 그리고 경고/로깅 과정을 단계적으로 거치게 된다. 이때 하나의 패킷처리가 완료된 후 다음 패킷이 처리된다. Pcap 라이브러리를 이용해서 패킷을 캡처하는데 Pcap의 특성상 처리속도가 늦어지면 캡쳐된 패킷은 버려진다. 즉, 패킷캡쳐 후

처리속도가 중요하다.

2.2 다중 쓰레드 기반 Snort 시스템

표준 Snort에서 경고 처리 성능을 향상시키기 위해서 Syed Yasir Abbas는 다중 쓰레드 기반으로 Snort를 수정하였다[2][4]. 단일 프로세스인 Snort에서 경고처리부분을 다중 쓰레드로 분리해 주 프로세스의 부하를 감소시키려 한 것이다. (그림 2)는 높은 디스크 지연 오버헤드가 있거나 네트웍 지연이 발생될 경우 경고처리를 위한 부분 때문에 Snort 전체 프로세스에 영향이 있다고 판단하여 재구성하였다.

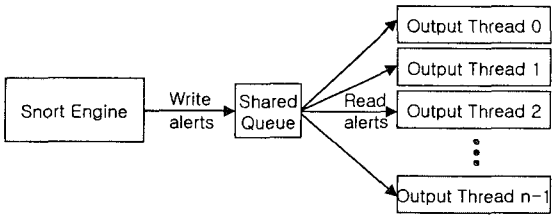

그림 2. 다중 쓰레드 모델
Figure 2. Multi-Thread Model

Syed Yasir Abbas 는 단일 쓰레드로 구성된 모델과 다중 쓰레드로 구성된 모델에 부하를 주어 해당 경고처리하는데 소요시간을 측정하여 성능평가 하였다[2].

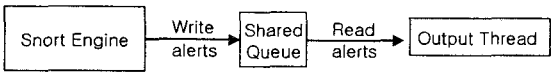

그림 3. 단일 쓰레드 모델 (표준 Snort)
Figure 3. Single-Thread Model(Standard Snort)

경고를 처리하기 위해 텍스트 파일에 쓰는 것만 테스트하였다. 그럼에도 불구하고 다중 쓰레드방식으로 처리할 때 성능이 향상되었음을 결과로 얻었다. 실험결과를 정리하면 부하가 많고 경고처리 해야 할 메시지가 많아진다면 쓰레드 개수를 늘리면 된다. 그리고 부하가 적고 경고처리 해야 할 메시지가 적어진다면 쓰레드 개수를 줄이면 된다. 쓰레드 개수의 튜닝은 각각의 환경에서 실험을 통해 얻어야하며 이는 성능의 결정적인 역할을 한다. Syed Yasir Abbas가 제안한 모델은 실제 발생된 경고처리능력을 향상시킬 수 있다. 그러나 네트웍기반 침입탐지시스템의 탐지 성능향상이 아니라 프로세스의 처리성능 향상이다. 현실적으로 잘못된 경고가 많이 발생되는 침입탐지시스템에서 무조건 많은 경고를 처리했다고 전체적인 성능이 좋아진다고 볼 수는 없다. 과다한 경고메시지로 인해서 실제 서비스 거부 공격이 될 수 있고 실제 공격을 구분해 내기도 어렵다. 이를 해결하기 위해서는 잘못된 경고를 줄이거나 경고 메시지를 축약하는 등의 기본 탐지프로세싱 구조를 변경해야한다. 본 논문에서는 기존 Snort의 경고처리성능을 향상시킨 Syed Yasir Abbas의 모델에 선행처리부분과 탐지처리부분을 분리하여 새로운 다중 쓰레드 모델을 제안한다. 이 모델은 상호 연관성 분석 모듈과 함께 웹서버 보안관리 시스템의 처리능력을 향상시킨다.

2.3 상호연관성 분석 기법

상호연관성 분석(Correlation Analysis) 또는 연계분석 개념은 예전부터 있었지만 요즘 보안이 이슈가 되면서 특히 통합보안관리시스템(ESM: Enterprise Security Management)이 시장에서 활기를 띠면서 국내외에서 가장 큰 기술적인 이슈로 떠오르고 있다[8].

이에 대한 개념을 알아보고 필요한 부분을 웹서버 보안관리시스템을 설계하는데 접목시킨다. 먼저 상호연관성 분석 개념은 통합보안관리측면에서 보면 다양한 이기종의 단위보안제품에서 발생하는 이벤트간의 연관관계를 분석하여 침해사고 또는 이와 관련된 의심스러운 행위를 분석하는 보안관리의 주요 요소라고 할 수 있다. 최근의 침해사고들을 분석해보면 최초 15분 이내에 적절한 대응을 하지 못할 경우 심각한 피해를 입을 수 있는 사례들이 빈번해지고 있으며 이를 사전에 탐지할 수 있는 방법으로 실시간 상호연관성 분석이 강조되고 있다. 데이터베이스에 저장되어있는 데이터를 가지고 분석하는 기법은 비실시간으로 탐지하는데 어려움이 있고 제한적이 된다.

단위보안제품들을 이용한 상호연관성 분석 예를 들어보면 다음과 같다.

▷ 두 가지 디바이스간의 관계적 요소 분석

네트웍 트래픽이 임계치 값을 초과하고 동일 시간대에 트래픽을 유발하는 바이러스가 발생된 경우 상호연관성 분석

▷ 두 가지 디바이스간의 인과적 요소 분석

침입탐지 시스템에서 불법접근시도 이벤트가 탐지되고 그때 동일한 근원지 IP, 목적지 IP와 관련된 방화벽의 이벤트가 거부(또는 허용)된 경우 상호연관성 분석

▷ 세 가지 디바이스간의 인과적 요소 분석

침입탐지 시스템에서 불법접근시도 이벤트가 탐지되고 그때 동일한 근원지 IP, 목적지 IP와 관련된 방화벽의 이벤

트가 허용되고 해당 목적지 시스템의 주요 파일변조가 발생된 경우 상호연관성 분석

▸ 동종의 여러 디바이스의 통계적 요소 분석

모든 침입탐지 시스템 (혹은, 안티바이러스)에서 동일한 유형의 침입패턴(또는 바이러스)이 30초 동안 5회 이상 발견되는 경우 상호연관성 분석

현실적으로 실시간 상호연관성 분석의 경우 많은 제약이 있다. 먼저 이기종간의 이벤트들을 비교해야 하기 때문에 그들의 공통 요소를 찾아 상호간 연관관계를 맺어야 한다. 실시간 처리이기 때문에 초당 수천, 수만 건의 이벤트들을 모두 처리할 수 있는 구조가 되어야 한다. 그리고 이러한 규칙에 의해 탐지된 결과는 의미가 있어야 하며 잘못된 경고를 감소시켜야 한다.

III. 웹서버 보안관리시스템 설계

3.1 네트웍기반 침입탐지시스템 구조

본 논문에서 제안한 웹서버 보안관리시스템의 성능에 많은 영향을 주는 단위보안모듈이 네트웍기반 침입탐지시스템이다. 관련연구에서 Snort는 공개소스로 널리 사용되는 네트웍기반 침입탐지시스템이기 때문에 Snort를 이용하여 재구성한다. Syed Yasir Abbas는 다중 쓰레드 기반으로 Snort구조를 변경하여 처리속도 향상을 했는데, 본 논문에서는 보다 좀 더 빠른 처리성능을 갖도록 새로운 모델을 제시한다.

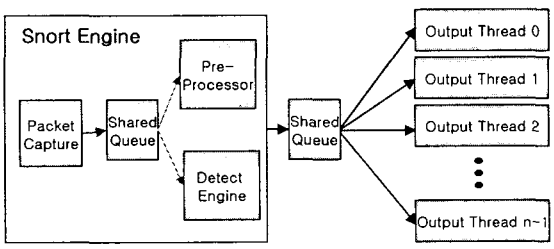

그림 4. 제안하는 네트웍기반 침입탐지시스템 구조
Figure 4. Architecture of suggests NIDS

(그림 4)는 단위보안모듈 중 네트웍기반 침입탐지시스템은 Snort 엔진부분을 두개의 쓰레드로 분리하여 엔진부분에서부터 처리속도를 향상시킬 수 있는 구조로 재설계했다. 현재 Snort는 선행처리 모듈과 탐지 모듈이 순차적으로 처리된다. 제안하는 네트웍기반 침입탐지시스템은 이 부분을 별도의 쓰레드로 분류하고 쓰레드간의 인터페이스 방법으로 원형 큐를 중간에 두어 디코드된 패킷을 원형 큐에서 두개의 쓰레드가 공유하게 된다. Snort의 순차적 처리를 병행처리로 가능하게 되고 탐지속도를 향상시킨다.

3.2 웹서버 보안관리시스템 구조

관련 연구와 제안한 단위보안 모듈인 네트웍기반 침입탐지시스템을 활용하여 웹서버 보안 관리시스템을 설계한다. 웹서버의 보안을 강화하기 위해 네트웍기반 침입탐지시스템, 시스템 로그, 파일 무결성, 웹 로그 모듈의 단위보안 모듈의 기능을 추가하여 실시간으로 웹 서버의 상태와 웹 서비스를 검사하고 경보를 발생시켜주는 시스템이다. 대규모의 통합 보안관리시스템을 웹서버에 맞도록 최적화 시킨 시스템이라고도 할 수 있다. 웹 서비스에 대한 공격을 탐지하기 위해 침입패턴 기반의 침입탐지시스템이 사용되며 웹서버 시스템에 대한 상태를 파악하기 위해서 시스템 로그와 웹서버 로그가 이용되고 웹 서비스에 중요한 파일 변조를 검사하기 위해 파일 무결성 검사기가 이용된다.

이러한 여러 단위보안 모듈들을 동시에 운영하면서 통합적으로 관리하고 이벤트를 분석하기 위한 상호연관성 분석기 모듈이 이용되며 웹서버 보안관리시스템에 적합하도록 재설계된다. 먼저 웹서버 보안관리시스템의 전체적인 프레임워크와 각 모듈별로 사용되는 이벤트를 정규화하고 처리하기 위한 정규화 방법을 설명하며, 이를 기반으로 설계한 이벤트 수집기 설명한다. 그리고 정규화 되어 수집된 이벤트들은 그 자체로도 의미 있는 값이지만 이벤트들간의 연관성을 부여하여 이벤트 상호간을 분석하기 위한 상호연관성 분석기를 설계한다. 그리고 상호 연관성 분석 경보 설정을 위한 환경 파일 설정규칙을 설명한다.

(그림 5)는 제안하는 웹서버 보안관리시스템의 전체 프레임워크이다. 현재는 4가지 독립적인 보안모듈이 운영되면서 발생된 이벤트를 가지고 처리하게 된다. 이때 이벤트 정규화 방법이 이용되고, 그리고 정규화 되어진 이벤트들을 상호연관성 분석기가 미리 정의된 규칙에 의해서 분석하고 경보를 발생시키게 된다. 제안한 프레임워크를 보면 모듈을 쉽게 추가할 수 있으며, 또한 추가된 모듈에서 발생한 이벤트를 상호연관성 분석기 모듈에 추가하기가 용이한 확장성이 있다. 또한 제거하기도 용이하다.

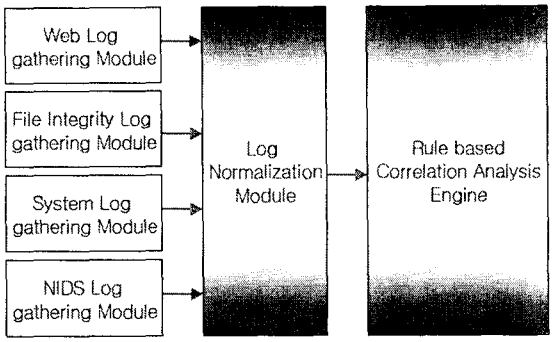

그림 5. 웹서버 보안관리시스템 프레임워크
Figure 5. Framework of WSM System

3.2.1 WSM 이벤트 정규화 방법

독립적인 모듈들에서 발생되는 이벤트는 정규화가 필요하며 정규화 방법을 설명한다.

표 1. 웹로그 정규화
Table 1. Normalization of Web Log

항목명	설 명
Origin IP	접속근원지 IP
Date	접속 날짜
Time	접속 시간
User	사용자 ID
Query	패스와 요구한 스트링
Protocol	사용되는 프로토콜
Status Code	서버 처리결과값
URL	접속 URL
Browser	클라이언트 브라우저 정보

아파치 웹서버의 로그파일 중 access_log 파일을 이용한다. access_log 파일에는 웹서버가 처리한 모든 Request들이 기록된다. 또한 내부지시자를 통해 필요한 내용들만 로그에 기록할 수도 있다.

표 2. 파일 무결성 정규화
Table 2. Normalization of File Integrity

항목명	설 명
Origin IP	IP (시스템 자신)
Date	변경 날짜
Time	변경 시간
File Name	파일명
Action	변경내용 (Update/Create/Delete)

파일 무결성 모듈은 공개소스 TripWire를 이용하여 미리 설정한 환경설정 파일에 의해 동작한다[10]. 미리 지정한 파일에 대해서 설정한 주기(1분 단위)로 그 파일 상태를 검사하고 변경/삭제/생성 의 작업이 이루어졌다면 이를 로그로 기록하게 된다. 이때 WSM에서 필요한 정보만을 가져와 〈표 2〉와 같은 포맷으로 정규화한다.

표 3. 시스템 로그 정규화
Table 3. Normalization of System Log

항목명	설 명
Origin IP	접속 근원지 IP
Date	접속 날짜
Time	접속 시간
User	사용자 계정
Level	Error/Warning/Information
Type	Login/User Right Change /Application
Information	Success,Fail,Log off/Ftp connect, disconnect,fail/user -> user /Application Name

시스템 로그는 기본적으로 시스템의/var/log/messages 파일을 사용하고 로그인 관련 로그, FTP, Telnet, 사용자 변경 등의 시스템 접속관련 로그를 정규화 하여 기록하게 된다. 그 외에도 어플리케이션에서 발생되는 로그를 기록하고, 시스템에서 현재 어떤 사용자가 로그상태 이며, 어떤 어플리케이션이 실행/종료 상태인지를 실시간으로 감시하게 된다. 단, 시스템 및 어플리케이션에서 syslog 형태로 로그를 남길 경우만 messages 파일에 저장된다.

표 4. 네트워크기반 침입탐지시스템 로그 정규화
Table 4. Normalization of NIDS Log

항목명	설 명
Origin IP	접속 근원지 IP
Date	접속 날짜
Time	접속 시간
Source IP	공격자 IP
Source Port	공격자 Port
Destination IP	목적지 IP
Destination Port	목적지 Port
Signature	공격 Signature
Protocol	프로토콜
Priority	레벨
Information	기타 정보

시스템 로그 정규화 내용을 보면 타입에 따라서 항목에 기록되는 값들이 달라진다. 즉 사용자 로그인 타입에 따라 성공, 실패, 로그오프가 기록될 수 있다. FTP의 경우는 접속, 연결끊기, 실패가 기록 되고, 사용자 변경 타입에서는 어떤 사용자에서 어떤 사용자로 변경했는지 여부가 기록된다. NIDS는 snort의 경고 로그파일을 이용한다. 이 로그내용을 위 정규화 포맷에 맞도록 필요한 정보만 저장하고 사용된다.

3.2.2 상호연관성 분석 모듈 설계

로그 정규화 모듈에서 정규화 된 이벤트들은 미리 정의된 규칙에 의해서 분석된다. 이때 분석하는 모듈을 상호연관성 분석기라 명명한다. 이벤트간의 공통의 요소를 Relation이라 명명하고 Relation과 Event Priority를 가지고 분석하게 된다.

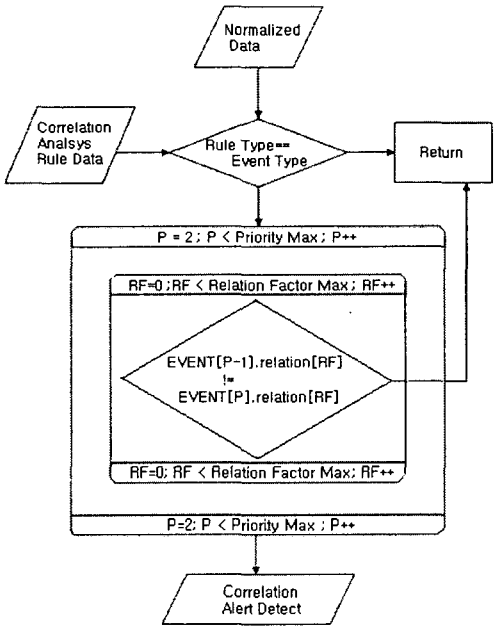

그림 6. 상호연관성 분석기 흐름도
Figure 6. Correlation Analysis Engine Flow Diagram

제안한 시스템에서는 4가지 보안모듈의 데이터가 수집되어지고 정규화 된다. System Event, Apache Log, File Integrity Log, NIDS Log이며, 이중에 공통된 요소 즉, Relation을 만들 수 있는 요소는 OriginIP, DATE, TIME이 된다. (그림 6)은 제안하는 상호연관성 분석기의 흐름도이다. 먼저 정규화 된 데이터가 정의된 경보 규칙에 있는지 검사한다. 그리고 경보 규칙의 우선 순위가 높은 데이터와 그 다음 이벤트 데이터의 해당 Relation을 갖는 데이터가 있는지 검사한다. 그래서 해당 Relation 관계가 있는 만큼 반복하며 비교한다. 우선 순위가 가장 높은 데이터부터 제일 낮은 데이터까지 반복해서 비교하게 된다. 이렇게 해서 해당된다면 경보 규칙에 맞는 데이터가 되며 경보를 발생시킨다.

3.2.3 상호연관성 분석 경고 설정 스크립트

상호 연관성 분석기를 통해 경보(Alert)를 상호연관성분석기에 인식시켜야 한다. 이를 위해 사용되는 방법이 경보 설정 스크립트이다. 가독성을 증가시키기 위해 간단히 표기를 했으며 향후 확장성을 고려해서 만들었다. 즉, Device라고 표시된 모듈들이 계속 추가된다고 해도 쉽게 추가할 수 있다. 위에 정의된 필드들을 설명하면 다음과 같다. AlertID는 설정한 경보를 구분할 수 있는 길이 10의 문자열이다. 일단 생성규칙은 A로 시작하고 2자리 년도, 2자리 월, _4자리 일련번호를 조합해서 구분한다. AlertLevel은 해당 경고 중요도에 따라 1부터 3까지 지정할 수 있다. AlertMessage는 해당 경보가 탐지 되었을 때 보여주는 문자열이 된다. 그리고 AlertDevice 에는 해당 경보규칙에서 연계분석하게 되는 Device 이름을 기술하며 아래에 해당 Device들이 우선순위별로 규칙이 지정되어야 한다.

```
#WSM Correlation Analysis Rule
#2004/08/18

AlertID = A0408_0001;
AlertLevel = 1;
AlertMessage=" Correlation Alert Detected!!!"
#(AlertNotify=DB,SMS;)

AlertDevice=SYSTEM,WEB
DeviceType=SYSTEM;
DevicePriority=1;
DeviceFilter=Login,User_right,Application;
DeviceRelation=OriginIP;

DeviceType=WEB;
DevicePriority=2;
DeviceFilter=404;
DeviceRelation=OriginIP;
```

그림 7. 경보설정 스크립트
Figure 7. Alert Configuration Script

DeviceType은 해당 모듈명이 지정되고 DevicePriority는 해당 모듈의 비교우선순위가 지정된다. 그리고 DeviceFilter는 모듈마다 다르게 지정되는데 SYSTEM 모듈의 경우 비교해야 할 값들은 Login, User right Change,

Application 항목들 모두 수집 비교한다는 뜻이다. DeviceRelation 필드는 현재 모듈의 결과와 다음우선순위 모듈과 비교하는 공통 요소를 지정한다. OriginIP라 지정이 되었다면 현재 SYSTEM의 OriginIP와 동일한 값을 가지는 데이터를 비교한다.

WEB 모듈의 경우는 웹서버가 Request 를 처리하고 리턴해 주는 값을 필터링 한다. 즉 404 와 같은 값들이다. 침입탐지시스템의 경우 Signature에 들어가는 문자열을 필터링 하게 된다. FILE_INTEGRITY 는 UPDATE, CREATE, DELETE 값들을 필터링 해서 비교한다.

Ⅳ. 네트워기반 침입탐지시스템 성능평가

네트워기반 침입탐지시스템은 표준 Snort(단일 쓰레드)와 Syed Yasir Abbas가 제안한 다중 쓰레드 모델, 그리고 본 논문에서 제안한 모델에서 경고처리 속도를 비교한다. 경고를 발생시키기 위해 "Ping ?s 1 ?n k ipaddress " 와 같은 악의적인(malicious ping) 공격을 사용한다.

모두 4대의 장비에서 Malicious Ping 공격을 하는데 공격 방법은 지정한 개수만큼 Ping 프로세스를 fork해서 동시에 Ping 공격을 하도록 프로그램을 작성해서 이용한다. 그리고 성능평가 척도는 지정한 개수의 경고를 탐지 할 때까지 소요된 시간을 비교한다. 여러 번 다양한 변수를 주어 성능평가를 하였으며 그 중에 대표적인 두 가지를 설명한다.

〔성능평가 1〕

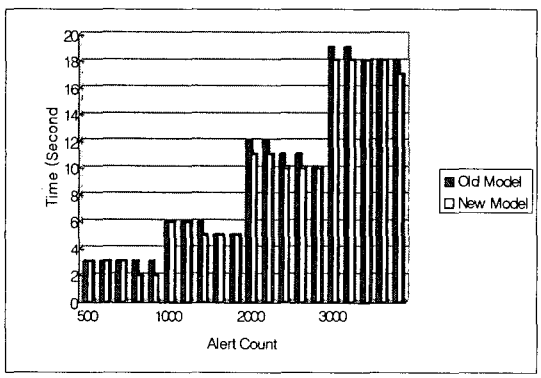

그림 8. 성능 평가 1
Figure 8. Performance Evaluation 1

Old Model 은 Syed Yasir Abbas가 제안한 모델이고, 이때 쓰레드 수가 1일 경우는 표준 Snort를 말한다. 그리고 New Model은 본 논문에서 제안한 새로운 다중 쓰레드 기반 침입탐지시스템이다. 쓰레드 개수를 10, 20, 50, 100으로 증가시켜가면서 지정한 경고 개수만큼 처리될 때까지 시간을 초단위로 비교하였다. 전체적으로는 New Model이 Old Model 보다 처리 성능이 빨라졌음을 확인할 수 있다. Old Model이 이미 표준 Snort를 다중 쓰레드기반으로 성능을 향상 시켰음을 감안한다면 New Model은 이보다 더 많은 성능 향상이 있음을 확인할 수 있다.

결과적으로 쓰레드 개수가 많아지면 성능도 향상되었고 그리고 경고의 수가 많을수록 즉, 측정시간을 증가시켜도 성능의 향상은 균일하게 나타났다.

〔성능평가 2〕

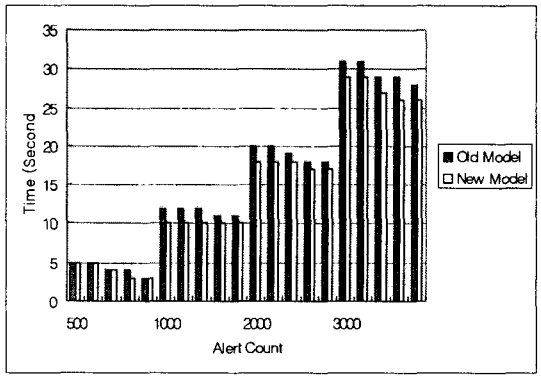

그림 9. 성능 평가 2
Figure 9. Performance Evaluation 2

〔성능평가 2〕는 〔성능평가 1〕 보다 공격 프로세스 개수를 2배로 하여 평가하였다. 〔성능평가 1〕과 비슷한 결과를 나타낸다. 즉 동일한 처리를 할 때 쓰레드 수가 많아지면 처리속도가 빨라지고 Old Model 보다 제안한 New Model이 약간의 성능향상이 있음을 알 수 있다. 구조적으로 선행처리 모듈과 탐지모듈을 서로 다른 쓰레드로 분리함으로서 병행처리 할 수 있게 되었다. 이로 인해 성능의 개선을 가져왔으며 본 논문에서 제안하는 웹서버 보안관리시스템에도 성능 개선을 보인다.

V. 웹서버 보안관리시스템 운영 시나리오 및 결과

본 논문에서 제안한 웹서버 보안관리시스템을 운영하고 상호연관성 분석을 통해 경고메시지 만드는 과정을 시나리오를 통해 검증해보도록 한다. 즉 잘못된 경고를 줄이고 확실한 증적이 있을 경우에만 경고를 발생시켰음을 실제 시나리오를 통해 증명한다.

〔시나리오 1〕 웹 서버 로그에 404 에러가 발견되고 이때 CGI 스캔 공격이 탐지되었을 경우 상호연관성 분석

웹서버 로그
192.168.10.128 [17/Aug/2004:16:23:00 +0900] "HEAD /cgi-bin/webdist.cgi HTTP/1.0" 404 0

침입탐지시스템 로그
[**] [1:1163:10] WEB-CGI webdist.cgi access [**] [Classification: access to a potentially vulnerable web application] [Priority: 2]
08/17-16:23:00.494309 192.168.10.128:1392 -> 192.168.10.24:80
TCP TTL:128 TOS:0x0 ID:31643 IpLen:20 DgmLen:203 DF
AP Seq: 0xD9870DDC Ack: 0xA37BA142 Win: 0xFFFF TcpLen: 20
[Xref =>] http://cgi.nessus.org/plugins/dump.php3?id=10299 [Xref =>] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0039 [Xref => http://www.securityfocus.com/bid/374]

상호연관성 분석기 로그
Correlation Alert [A0408_0001]
2004/08/17 16:23:00 "webdist.cgi Scan Detect !!!"
Alert Device : Web, NIDS
Detail Log of Web [Priority 1]
192.168.10.128 2004/08/17 16:23:00 "HEAD /cgi-bin/webdist.cgi HTTP/1.0" 404 0
Detail Log of NIDS [Priority 2]
192.168.10.128 2004/08/17 16:23:00 "WEB-CGI webdist.cgi access" TCP Priority: 2
[Classification: access to a potentially vulnerable web application]

네트웍기반 침입탐지시스템 로그와 웹서버 로그가 동시에 연관성이 있을 경우 경고가 발생된다. 즉, 아래와 같이 발생이 되었을 경우 경고가 발생된다. 웹로그와 침입탐지시스템모듈 원시로그가 보이고 그 다음 상호연관성 분석을 통해 만들어진 경고와 정규화 된 상세로그가 보여진다.

〔시나리오 2〕 네트웍기반 침입탐지시스템에서 스캔공격이 탐지되고, 그 시간에 시스템 로그에 Telnet 접속과 사용자 변경이 발생되었으며 그 시간에 파일 무결성 모듈에서 웹 서비스 주요파일이 변경된 경우 상호연관성 분석

침입탐지시스템 로그
[**] [1:716:9] TELNET access [**]
[Classification: Not Suspicious Traffic] [Priority: 3]
08/17-19:06:14.298727 192.168.10.24:23 -> 192.168.10.128:3635
TCP TTL:64 TOS:0x0 ID:18851 IpLen:20 DgmLen:52 DF
AP Seq: 0x167010B7 Ack: 0x75AA8FC1 Win: 0x7D78 TcpLen: 20
[Xref =>] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0619 [Xref => http://www.whitehats.com/info/IDS08]

시스템 로그
Aug 17 19:06:08 localhost PAM_pwdb[29680]: (login) session opened for user ccuser by (uid=0)
Aug 17 19:06:14 localhost PAM_pwdb[29696]: (su) session opened for user root by ccuser (uid=500)

파일 무결성 로그
2004-08-17 19:06:14 [File Integrity] U 0 0 0 0 /home/root/public_html/index.html 0

상호연관성 분석기 로그
Correlation Alert [A0408_0002]
2004/08/17 19:06:14 "Web Sevice Attack Detect !!!"
Alert Device : NIDS, SYSTEM , File Integrity
Detail Log of NIDS [Priority 1]
192.168.10.128 2004/08/17 19:06:14 "TELNET access"
TCP Priority: 3
[Classification: Not Suspicious Traffic]
Detail Log of SYSTEM [Priority 2]
192.168.10.128 2004/08/17 19:06:08 Login, ccuser
192.168.10.128 2004/08/17 19:06:14 User Right change, ccuser -> root
Detail Log of File Integrity [Priority 3]
192.168.10.128 2004/08/17 19:06:14 UPDATE "/home/root/public_html/index.html"

침입탐지시스템에 의심스러운 공격이 아니라고 탐지되었지만 결과 내용으로 봐서는 웹 서비스의 치명적 손상을 줄 수 있는 행위들이다. 이러한 이기종간의 활동들을 실시간으로 상호 연관성 분석을 한다면 공격자가 들어와서 로그를 지우는 행위를 하더라도 이전에 이미 탐지되어 경고가 발생된다.

Ⅵ. 결 론

본 논문에서는 웹 서비스와 같은 특정 시스템에 대해서 비용과 관리의 증가 없이 정확하고 빠르게 공격을 탐지 할 수 있고, 잘못된 공격탐지를 줄일 수 있는 웹서버 보안관리 시스템을 제안하고 구현하였다. 특정시스템을 위해 모든 단위보안제품을 이용하는 것은 비용과 관리적인 측면에서 너무 많은 손실이 있다. 제안한 웹서버 보안관리시스템은 비용적인 측면을 감소하기 위해 공개소스기반의 단위보안모듈들을 이용하였고, 관리적인 문제를 해결하기위해 상호연관성 분석 모듈을 이용하였다. 또한 전체적인 시스템의 성능을 향상시키기 위해 제일 부하가 많은 단위보안모듈인 네트웍기반 침입탐지시스템을 다중 쓰레드 기반으로 재설계하여 이용하였다. 즉, 선행처리 모듈과 탐지 모듈을 분리했다. 이로써 웹서버 보안관리시스템 전체 성능을 향상시킬 수 있었다. 결과적으로 웹서버 보안관리시스템은 현재 웹서버 시스템에 전문적인 보안 관리자 없이도 웹서버 시스템을 보다 안전하고 추가 비용 없이 관리 운영하도록 도와준다. 특히 다양한 이벤트간의 상호연관성 분석 모듈은 웹서버 보안관리시스템의 핵심 기능이며 구조적으로 쉽게 추가 모듈을 장착하여 상호연관성 분석의 범위를 늘려가기 용이한 프레임워크를 제공한다.

향후에는 이러한 프레임워크를 기반으로 자신의 취약점을 진단할 수 있는 취약점 진단 모듈, 그리고 트래픽의 상황을 실시간 감시할 수 있는 트래픽 감시 모듈 등을 추가하여 상호연관성 분석 모듈에 장착한다면 보다 안전한 웹 서비스와 웹서버 시스템을 만들 수 있을 것이다.

참고문헌

[1] "2003 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY", Computer Security Institute, 2003

[2] Syed Yasir Abbas, "Introducing Multi Threaded Solution to Enhance the Efficiency of Snort", Florida State Univ, MS thesis, 2002. 12

[3] Deron Powell, "Enterprise Security Management (ESM): Centralizing Management of Your Security Policy", SANS Info, 2002. 12

[4] Jay Beale, James C. Foster, Jeffrey Posluns, Brian Caswell, "Snort 2.0 Intrusion Detection", Syngress Publishing, 2003

[5] 차병래, 박경우, 서재현, "이상 침입탐지를 위한 베이지안 네트워크 기반의 정상행위 프로파일링", 한국컴퓨터정보학회 논문지, 제 8권 1호, 2003. 3

[6] 최양서, 최병철, 서동일, "OpenSource 를 활용한 S-ESM개발", 한국전자통신연구원 사이버테러기술분석팀, JCCI, 2003. 4

[7] 최인수, 장덕성, "침입탐지 시스템의 성능향상을 위한 버퍼구조에 관한 연구", 한국컴퓨터정보학회 논문지, 제 8권 2호, 2003. 6

[8] 이글루시큐리티, http://www.igloosec.co.kr

[9] Snort.org, http://www.snort.org

[10] Tripwire.org, http://www.tripwire.org

저 자 소 개

김 성 락

1984년 울산대학교 전자계산학과 (학사)

1989년 한양대학교 산업대학원 전자계산학전공(석사)

2003년 수원대학교 대학원 전자계산학과(박사)

1996년 ~ 현재

오산대학 인터넷정보과 부교수